NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ARCHITECTING A NET-CENTRIC OPERATIONS SYSTEM OF SYSTEMS FOR MULTI-DOMAIN AWARENESS

by

Keith L. Ruegger

September 2008

Thesis Advisor:	Thomas V. Huynh
Co-Advisor:	John S. Osmundson

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2008	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Architecting a Net-Centric Operations Systems of Systems for Multi-Domain Awareness		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Keith L. Ruegger			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

Maritime domain awareness (MDA) entails knowing what is happening in the oceans and waterways that could affect the security or environment of the United States. With a focus on potential attack vessels (PAV) as threats in the maritime domain, a multi-domain SoS is needed to exploit and integrate information from multiple sources, including sensors, databases, and intelligence, to provide reconnaissance, surveillance, and information used in the formulation of a common operational picture (COP), a tool to effect maritime domain awareness. In this thesis the best architecture of net-centric operations (NCO) multi-domain system of systems (SoS) for MDA is determined, employing an integrated systems engineering methodology for analyzing and ranking systems of systems architectures.

This methodology involves the use of process modeling, modeling of an SoS with the systems modeling language (SysML), and subsequent conversion of the resulting SysML diagrams into an Extend™ executable simulation model, used in a simulative study carried out to evaluate three multi-domain awareness SoS architecture alternatives in terms of the time to establish a COP and the probability of COP accuracy.

Of the three architecture alternatives, a conceptual SoS whose constituting systems are connected in a distributed network with a high degree of connectivity is found to take the least amount of time to establish a COP and to have a high probability of COP accuracy. It can thus be considered to be the best of the three MDA SoS architecture alternatives.

The results indicate that, in a distributed network, which is the backbone of net-centric operations, direct links between the sensors and the coalition C2 center shorten the communications delay and hence reduce the time to establish a COP. The accuracy of the information to be combined at the coalition C2 center is necessary for having a high probability of COP accuracy. Furthermore, the integrated systems engineering methodology for analyzing SoS architectures provides an effective framework and tool for designing and analyzing complex SoS in general and NCO MDA SoS in particular.

14. SUBJECT TERMS System of Systems, SoS, Net-Centric Operations, NCO, Multi-Domain Awareness, Maritime Domain Awareness, MDA, SoSADP			**15. NUMBER OF PAGES** 103
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ARCHITECTING A NET-CENTRIC OPERATIONS SYSTEMS OF SYSTEMS FOR MULTI-DOMAIN AWARENESS

Keith L. Ruegger
Lieutenant Commander, United States Navy
B.S., United States Naval Academy, 1991
M.S., Naval Postgraduate School, 1999

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2008

Author: Keith L. Ruegger

Approved by: Thomas V. Huynh, Ph.D.
Thesis Advisor

John S. Osmundson, Ph.D.
Thesis Co-Advisor

David H. Olwell, Ph.D.
Chairman, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Maritime domain awareness (MDA) entails knowing what is happening in the oceans and waterways that could affect the security or environment of the United States. With a focus on potential attack vessels (PAV) as threats in the maritime domain, a multi-domain system of systems (SoS) is needed to exploit and integrate information from multiple sources, including sensors, databases, and intelligence, to provide reconnaissance, surveillance, and information used in the formulation of a common operational picture (COP), which is a tool to effect maritime domain awareness. In this thesis, the best architecture of net-centric operations (NCO) multi-domain SoS for MDA is determined, employing an integrated systems engineering methodology for analyzing and ranking systems of systems architectures.

This methodology involves the use of process modeling, modeling of an SoS with the systems modeling language (SysML), and subsequent conversion of the resulting SysML diagrams into an Extend^{TM} executable simulation model used in a simulative study conducted to evaluate three multi-domain awareness SoS architecture alternatives in terms of the time to establish a COP and the probability of COP accuracy.

Of the three architecture alternatives, a conceptual SoS whose constituting systems are connected in a distributed network with a high degree of connectivity, is found to take the least amount of time to establish a COP and to have a high probability of COP accuracy. It can thus be considered to be the best of the three MDA SoS architecture alternatives.

The results indicate that, in a distributed network, which is the backbone of net-centric operations, direct links between the sensors and the coalition C2 center shorten the communications delay, and hence, reduce the time to establish a COP. The accuracy of the information to be combined at the coalition C2 center is necessary for having a high probability of COP accuracy. Furthermore, the integrated systems engineering methodology for analyzing SoS architectures provides an effective framework and tool for designing and analyzing complex SoS in general and NCO MDA SoS in particular.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

There are few areas of greater strategic importance than the maritime domain. Distinct from other domains (e.g., air and space), the maritime domain provides a global transit medium that sustains national prosperity and is vital to national security. In light of the possibility of terrorist activities, accidents, and natural disasters, maritime domain awareness (MDA) has emerged as a high-priority mission area in both the Department of Defense and the Department of Homeland Security. MDA entails knowing what is happening in the oceans and waterways that could affect the security or environment of the United States.

The purpose of this thesis is to architect a net-centric operations (NCO) multi-domain system of systems (SoS) for MDA. Focusing on potential attack vessels (PAV) as threats in the maritime domain, a multi-domain SoS is needed to exploit and integrate information from multiple sources, including sensors, databases, and intelligence, to provide reconnaissance, surveillance, and MDA.

This thesis employs the integrated systems engineering methodology for analyzing and ranking systems of systems architectures espoused in [3]. Developed at the Naval Postgraduate School, this methodology involves the use of process modeling, modeling of an SoS with the systems modeling language (SysML), and subsequent conversion of the resulting SysML diagrams into an SoS executable simulation model. This work explains the methodology, emphasizes the traceability between the SysML representation of a conceptual SoS and its Extend™ executable model, and then applies the methodology with an analysis of coalition SoS architecture alternatives to determine the best NCO multi-domain awareness SoS architecture.

Three architecture alternatives for a multi-domain awareness SoS are considered: A current architecture, a planned architecture, and a conceptual architecture. In all three architectures, the Coalition C2 center produces Common Operational Pictures (COP). A COP serves as a tool to effect maritime awareness. In the current architecture, Architecture #1, the coalition network allows communications between the Coalition

command and control (C2) center and each coalition nation C2 center, which communicates with its platforms/sensors via its respective nation's network, processes the raw data from its sensors, and transmits the information resulting from processing raw data from its sensors to the Coalition C2 center. The planned architecture, Architecture #2, is similar to Architecture #1, except that the Coalition C2 center communicates direct tasking assignments to a coalition nation's platforms/sensors without going through the respective host nation C2 center, which still processes the raw data from its sensors. For the conceptual architecture, Architecture #3, the Coalition C2 center communicates tasking assignments directly with the coalition sensors and processes the raw sensor data obtained directly from the coalition sensors, thereby eliminating the need for sensor data processing at the coalition nation C2 centers.

A simulative study is undertaken to evaluate the performance of the three multi-domain awareness SoS architecture alternatives. In this simulative study, three Extend™ models are created, implementing the SysML sequence diagrams for the three multi-domain awareness SoS architecture alternatives. The Extend™ models are designed specifically to represent the flow of messages and data that traverse the coalition C2 network in a specific sequence of events, called a thread. Five hundred simulation runs are made, whose results are processed to yield two measures of performance, the time to establish a COP and the probability of COP accuracy.

The first measure of performance, the time to establish a COP, is the difference between the start time of the thread's first event and the end time of the thread's last event. The first event occurs when an Intel alert is received by the Coalition C2 center. The last event occurs when the COP is received by all coalition nation C2 centers. A descriptive statistical analysis is performed on the simulation results, namely, the values of the time to establish a COP. The results of the statistical analysis show that Architecture #1, the current architecture, takes the longest time to establish a COP, with a mean time of 818 seconds. Architecture #2, the planned architecture, takes an average of 779 seconds to establish a COP, which is approximately 5% less than that of the current architecture. The conceptual architecture, Architecture #3, establishing a COP

with a mean time of 739 seconds, shows almost a 10% improvement over the current architecture. The best MDA SoS architecture that takes the least amount of time to establish a COP is thus Architecture #3. As time to establish a COP is reduced, coalition C2 centers receive shared information quicker, which facilitates collaboration and timely decision making.

The second measure of performance is the probability of COP accuracy. In reality, raw sensor data and/or processed sensor data are combined to form a COP. Consequently, the accuracy of a COP depends on that of the raw sensor data and/or processed sensor data. Since this research does not deal with raw or processed data from the coalition sensors or the coalition nation C2 centers, a simple probabilistic model is used to estimate the probability of COP accuracy. According to this probabilistic model, the accuracy of the information resulting from processing the sensor data at the coalition nation C2 centers or the coalition C2 center is conservatively assumed to be uniformly distributed between zero and one. The probability of COP accuracy is then taken to be the maximum value of the probability of accuracy of the information received from the coalition C2 centers or the information resulting from directly processing the coalition sensors.

The probabilistic analysis indicates that the probability of COP accuracy for both Architecture #1 and Architecture #2 is approximately 0.75. The first two architectures have the same probability since both architecture alternatives have the same number of data inputs used in the formation of a COP. Architecture #3, with a probability of COP accuracy of approximately 0.83, shows almost a 10% improvement over Architectures #1 and #2. The MDA SoS architecture alternative with the highest probability of COP accuracy is therefore Architecture #3. Finally, based on the two measures of performance, Architecture #3 can be considered to be the best of the three MDA SoS architecture alternatives.

Some key findings result from the research conducted in thesis. First of all, in general, in a highly distributed network, which is the backbone of net-centric operations, the resulting connectivity of the network would allow direct or assured communications with reduced delay between any two nodes of the network, provided that no bottleneck

resulting from lack of sufficient bandwidth exists on any communications link. In particular, in the distributed network of Architecture #3, direct links between the sensors and the coalition C2 center shorten the communications delay and hence reduce the time to establish a COP.

Second, the integrated systems engineering methodology for analyzing SoS architectures provides an effective framework and tool for designing and analyzing complex SoS in general and NCO MDA SoS in particular. Architecture representations using SysML activity and sequence diagrams aid in identifying and resolving some modeling and SoS interoperability issues, such as communications and concepts of operations. Furthermore, modeling the threads (i.e., sequences of events), based on these SysML diagrams, aids in understanding the NCO MDA SoS behavior.

Finally, the simulative study has been found to be an effective tool for assessing the performance of the SoS architectures and for ranking the SoS architectures. The results of this research are conservative; however, actual raw or processed sensor data may provide results that are more realistic.

ACKNOWLEDGMENTS

There are few people I would like to thank for helping me complete this thesis. The first is Dr. Thomas Huynh, my primary thesis advisor. Professor Huynh provided just the right encouragement and help whenever I asked. He makes student learning a top priority in his job and is always willing to take time out of his busy schedule to provide guidance. I enjoyed our many conversations and interesting discussions about various topics. I would also like to thank Dr. John Osmundson, my thesis co-advisor, for his help and insight. Finally, I want to thank my family and friends for their help and support.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> The heart of the Maritime Domain Awareness program is accurate information, intelligence, surveillance, and reconnaissance of all vessels, cargo, and people extending well beyond our traditional maritime boundaries [1].
>
> President Bush
> January 20, 2002

A. BACKGROUND

There are few areas of greater strategic importance than the maritime domain. The maritime domain is defined as "all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime related activities, infrastructure, people, cargo, and vessels and other conveyances" [1]. Distinct from other domains (e.g., air and space), the maritime domain provides expansive lines of communication that sustain global prosperity and are vital for global commerce. Terrorist organizations realize the maritime domain's economic importance and recognize the importance of exploiting the maritime domain as a medium for launching attacks. The maritime domain presents many potential targets that meet terrorists' objectives of achieving mass casualties and inflicting great economic damage.

Today's terrorist threats place an even greater premium on knowledge and shared understanding of the maritime domain environment. One of the most frightening terrorist threats involves terrorists smuggling and activating a weapon of mass destruction (WMD) using a container ship in a U.S. port. Such a catastrophic event would cause massive destruction and enormous economic damage, not to mention death to countless innocent people. In a 2003 study, the U.S. Department of Transportation concluded that a detonation of a nuclear weapon in a major U.S. port could cost between "hundreds of billions to trillions" of dollars in damages [2]. This scenario shows the staggering potential costs from a ship-borne, WMD terrorist attack. The stakes are extremely high, and preventing an attack of this magnitude precipitates the need for greater awareness and protection.

The key to preventing a maritime attack is situational awareness in the maritime domain and knowledge of maritime threats, along with deterrent and interdiction capabilities [1]. Situational awareness is derived from an effective understanding of domain activities, which depends on the ability to monitor activities to identify trends and anomalies. Situational awareness in the maritime domain is called maritime domain awareness (MDA). MDA entails knowing what is going on in the oceans and waterways that could affect the security or environment of the United States. All available data and information must be collected, analyzed, fused, and interpreted in order to be used to provide MDA enabling authorities to better anticipate and defeat maritime threats.

B. PURPOSE

The purpose of the research conducted in this thesis is to architect a net-centric operations (NCO) multi-domain system of systems (SoS) for maritime domain awareness. Focusing on threats from potential attack vessels (PAV) in the open ocean, multi-domain systems exploit and integrate information from multiple sources, including sensors, databases, and intelligence, to deliver reconnaissance, surveillance, and situational awareness to provide maritime domain awareness. By exploiting information from multiple sources and domains, the NCO multi-domain SoS provides the information and situational awareness needed to solve the challenges associated with maritime domain awareness. The multi-domain SoS attempts to integrate multiple sources from multiple domains to provide maritime domain awareness.

C. RESEARCH QUESTION

What is the best net-centric operations system of systems architecture for multi-domain awareness? This question shapes the research and analysis of this thesis.

D. SCOPE

This research is limited to NCO SoS architectures that focus on the multi-domain aspect of maritime domain awareness. It does not consider the political and diplomatic realms, assuming full international cooperation by all coalition partners, and it focuses on a generic, conceptual solution, with capabilities transferrable to other coalition problem areas.

E. BENEFITS OF STUDY

This research is important in that it contributes to the solution of the problem of architecting net-centric operations systems of systems architectures. Its results may apply to the multi-domain awareness efforts being pursued by the United States Joint Forces Command. Many of the processes and techniques discussed herein are applicable to integration and analysis efforts of complex systems architectures in any joint or large organization.

F. METHODOLOGY

The methodology used in this research is the integrated systems engineering methodology for analyzing architectures of NCO SoS espoused in reference [3]. Developed at the Naval Postgraduate School, the integrated systems engineering methodology is used to analyze and rank NCO SoS architectures for the multi-domain awareness mission. Developing an NCO SoS architecture starts with a problem in which a mission to be conducted by the SoS is stated and ends with a set of ranked SoS architectures [3]. The integrated systems engineering methodology involves linking the System of Systems Architecture Development Process (SoSADP) [3] with the development of Department of Defense Architecture Framework (DoDAF) products [4] and the use of systems modeling language (SysML) diagrams [5] in representing an SoS architecture. This methodology, discussed in Chapter II, will be applied to architecting a NCO SoS architecture for multi-domain awareness.

G. THESIS ORGANIZATION

This thesis is organized as follows. Chapter I provides an introduction to and an overview of the thesis, including the purpose, research question, scope, benefits, and methodology. Chapter II introduces the multi-domain awareness problem, including the background, problem statement, and scenario. It also introduces the elements of an SoS, including the platforms and sensors and command and control structures. Chapter III provides an overview of the integrated systems engineering methodology employed in this research, as well as brief descriptions and the interrelations between the SoS Architecture Development Process, DoDAF products, and SysML diagrams. In Chapter IV, the integrated systems engineering methodology is applied to produce representations of the alternative SoS architectures. Chapter V describes the simulative study along with the simulation models. It also contains the results, analysis, and recommendations. Finally, Chapter VI provides a summary of the research, as well as key findings, areas for future research, and conclusions.

II. MULTI-DOMAIN AWARENESS PROBLEM

A. INTRODUCTION

This chapter introduces maritime domain awareness (MDA), the net-centric operations (NCO) concept, and multi-domain systems of systems (SoS). The first section provides an understanding of what MDA entails and its goals and objectives. The second part describes the NCO concept and how it can be used to help with MDA. Finally, a multi-domain SoS is introduced as a way to achieve situational awareness in the maritime domain.

1. Maritime Domain Awareness

Maritime domain awareness is an area of strong interest to the United States and its allies. MDA spans a number of issues from missile defense and counterterrorism to cargo containers and shipping security, from drug trafficking and immigration to fishing rights and search and rescue [6]. MDA entails knowing what is going on in the oceans and waterways that could affect the security or environment of the United States. MDA's overarching goal is to increase global awareness and knowledge of what transpires in the maritime domain. Achieving this goal requires international and interagency communication and cooperation to integrate and share information and intelligence in all areas. Data collection is essential and must be accurate. Accuracy provides a filter for distinguishing normal behavior from unusual or anomalous behavior, sometimes indicative of the presence of threats in an MDA environment.

According to the National Security/Homeland Security Presidential Directive (NSPD-41/HSPD-13), Maritime Domain Awareness is defined as "the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the United States" [1]. MDA is a key component of a layered defense in depth approach that utilizes an integrated process to detect, identify, deter, and defeat the full spectrum of maritime threats. Defense in depth is a strategy that employs various mechanisms that increases protection by defending

against or preventing attacks. MDA is achieved by collecting, analyzing, fusing, displaying, and disseminating actionable information and intelligence to operational commanders. The following are the goals and objectives for MDA in accordance with the National Strategy for Maritime Security [1].

a. MDA Goals

Supporting core national defense and security priorities, MDA serves to simplify today's complex and uncertain security environment by achieving the following strategic goals:

- Enhance transparency in the maritime domain to detect, deter, and defeat threats as early and distant from U.S. interests as possible;
- Enable accurate, dynamic, and confident decisions and responses to the full spectrum of maritime threats; and
- Sustain the full application of the law to ensure freedom of navigation and the efficient flow of commerce.

b. MDA Objectives

Achieving MDA depends on the ability to monitor activities in such a way that trends can be identified and anomalies detected. The following objectives guide the development of capabilities needed to provide an effective understanding of the maritime domain environment and activities.

- Persistently monitor in the global maritime domain: Vessels and craft, cargo, vessel crews and passengers, and all identified areas of interest;
- Access and maintain data on vessels, facilities, and infrastructure;
- Collect, fuse, analyze, and disseminate information to decision makers to facilitate effective understanding; and
- Access, develop and maintain data on MDA-related mission performance.

MDA depends upon information sharing, and the method for information sharing is the use of a common operational picture (COP). The COP is a near real-time, dynamically tailored, network-centric virtual information grid shared by all organizations with maritime interests and responsibilities [1]. The ability to effectively track shipping is of critical importance to U.S. interests both at home and abroad. Every vessel must be

watched to determine if it poses a threat. The effective understanding of maritime domain activities enables effective decision making by authorities, and thereby, ensuring vital opportunities for an early response will not be lost. MDA is the critical enabler for national maritime security.

2. Net-Centric Operations Concept

The net-centric operations (NCO) concept is a product of the information age. It benefits from increases in computing power and technological advancements. The NCO concept employs a robust network environment (infrastructure, systems, processes, and people) to maximize data sharing, which is a key component of MDA. NCO relies on computer equipment and communications network technology to provide shared awareness of the battle space for military forces. The NCO concept proposes that "shared awareness increases synergy for command and control, resulting in superior decision-making, and the ability to coordinate complex military operations over long distances for an overwhelming war-fighting advantage" [7].

The Joint Chiefs of Staff recognized the advantages inherent in NCO and published the forward looking documents Joint Vision 2010/2020 [8], [9] incorporating the NCO concept into the future defense strategy. The Joint Vision documents detail how the United States Armed Forces will "leverage advancing technology to achieve unprecedented levels of power, timeliness, and decisiveness in joint operations and warfighting" [6]. The Joint Vision documents further detail how all future military operations will be 'joint,' including systems and forces contributing from all the Armed Services and from National agencies depending on circumstances. This document outlines the NCO operations concept including the fundamental role that information superiority plays in an organization's ability to prevail over its adversaries.

Following the release of the Joint Vision documents, all Department of Defense services independently developed and released conceptual descriptions of their future warfighting strategies, which supported the common themes presented by the Joint Chiefs of Staff. As a result, the U.S. Navy would shift its operational concept from one based on platform-centric warfare concepts to one based on net-centric warfare concepts. Net-

centric warfare is described as “a model of warfare that derives its power from a geographically dispersed force embedded within an information network that links sensors, weapons, and command and control nodes to provide increased speed of decision making, rapid synchronization of the force to meet desired objectives, and create economy of force” [10]. Ideally, net-centric warfare will deliver the right information to the right place at the right time to achieve a mission.

The U.S. Navy defines network-centric operations as “military operations that exploit state-of-the-art information technology to integrate widely dispersed human decision makers, situational and targeting sensors, and forces and weapons into a highly adaptive, comprehensive system to achieve unprecedented mission effectiveness” [10]. Although this definition is specific to the Navy, by removing the references to ‘military’ operations, this definition could apply to net-centric operations for any organization. The point of net-centric operations is to integrate an entire organization’s assets, or in this example a navel force, to maximize the effectiveness of its operations for success in accomplishing a goal or mission.

Since its introduction in the late 1990s, net-centric operations systems can be seen both in place and in the making throughout each service. However, this is just the start of creating net-centric operations systems to employ more efficient and effective assets. A net-centric operations system is a group of systems or sub-systems, designed and integrated, that operate effectively as a system of systems to accomplish a mission.

3. Multi-Domain System of Systems

There are many definitions for a system of systems (SoS). In this thesis, a SoS is an aggregation of existing, independent systems or to-be-defined and to-be-developed systems that are integrated and interoperable with each other. Two systems are interoperable if they can successfully exchange and process information in support of a task or a mission [3].

The U.S. has a formidable challenge when it comes to maritime security. A goal in maritime security is maritime domain awareness (MDA)—to know what and where an event is happening in the maritime domain or open-ocean approaches to the U.S. so that

potential threats can be dealt with as far away from the country as possible. In light of this formidable security challenge, all sensors can make an important contribution to identification and surveillance of potential threats. In fact, no single sensor is capable of providing complete surveillance or domain awareness; a combination of sensors or capabilities is therefore required. Since a capability or a sensor has strengths and weaknesses, the strongest surveillance architecture exists by combining multiple sensors in a complementary manner [11].

One way to achieve maritime domain awareness is through combining capabilities and sensors from multiple domains. Multi-domain awareness combines the capabilities and sensors from domains that may not normally share information with one another. As an example, a multi-domain awareness SoS would result from combining the Navy's ship-based sensors, the Air Force's airborne sensors, and national space-based sensors. This SoS would form a COP to aid authorities in better decision making. Another example is a multi-domain awareness SoS that would result from combining sensors from different coalition countries, such as Australian sensors, Canadian sensors, and American sensors; this SoS would form a single joint coalition COP. The goal is to create a multi-domain awareness SoS that supports the warfighter who does not have to worry about from where the information is coming, but knows information needs are being met with timeliness and precision [12].

B. MULTI-DOMAIN AWARENESS PROBLEM STATEMENT AND SCENARIO

1. Problem Statement

The statement of the multi-domain awareness coalition SoS problem may be simplified as follows: Architect an SoS consisting of capabilities, platforms, and sensors from coalition systems that will detect, track, and counter potential attack vessels (PAV) that potentially carry weapons of mass destruction (WMD) in open-ocean transit, before reaching their seaports of destination. Information and data from organizations

considered to be external to the SoS may be incorporated into the SoS to aid in multi-domain awareness. Example organizations considered external to the SoS include: intelligence, shipping companies, automated identification service (AIS), and weather.

2. Scenario[1]

Several seemingly disparate pieces of information are entered into an intelligence database. Intelligence tips from various coalition sources indicate a possible terrorist cell in Indonesia. Full motion video (FMV), received from human intelligence, shows a known terrorist, posing as part of a ship's crew, boarding a container ship (MV Alpha) in an Indonesian port. Another piece of human intelligence, photographs and FMV, shows cargo being loaded onto MV Alpha in New Guinea, along with sightings of known terrorists observing the cargo loading. When these pieces of information are viewed as independent events, there may not be enough evidence to make a connection or meet requirements for further action such as surveillance. However, when viewed from a holistic perspective, the connections among these pieces of intelligence become apparent and indicate a potential attack emanating from the sea by terrorists onboard a PAV with cargo of suspicious contents.

Intelligence information on suspicious container ships, along with their locations, is received by the Coalition Command and Control Center (CC2C). Requests for information from various external sources, such as AIS, shipping companies, and weather, are sent and received via the coalition network. The CC2C issues orders (with initial threat data) to the coalition nation command and control (C2) centers via the coalition network to track and monitor MV Alpha as a PAV. The Australian C2 center communicates with its platforms and sensors via the Australian network, the United States C2 center communicates with its platforms and sensors via the United States network, and the Canadian C2 center communicates with its platforms and sensors via the Canadian network. Each C2 center uses its distributed sensors (national, organic, and commercial) to monitor and track MV Alpha as a PAV.

[1] The scenario is similar to the scenario used in Empire Challenge 2006. Empire Challenge is a Joint/Allied interoperability demonstration series.

The coalition nation sensors collect all types of data including signals, measurements, imagery, and other tracking information. All the data collected by the distributed sensors networks from each coalition nation is processed, formatted, and sent via the coalition network to the CC2C to be integrated and fused into a COP. The COP is then disseminated to each coalition nation C2 center for every one in the coalition to view the COP. The COP provides a common picture of shared operational information facilitating MDA and aids in an effort to detect and track threats such as a PAV.

C. SYSTEM OF SYSTEMS COMMAND AND CONTROL

This section provides details of the command and control structure used in this research. A C2 structure determines the level of command, thereby establishing which platforms (C2 nodes) perform command and control functions. Orders initiate and reports terminate at the C2 nodes, which determine the flow of communications through the SoS architecture. In this research, three C2 structures are considered, which are discussed in detail in Chapter IV.

D. PLATFORMS AND SENSORS

A functional analysis leads to a functional architecture, which, embedded in platforms, leads to SoS compositions. Since the scope of this thesis is to present the analysis and simulation that enable selection of a multi-domain awareness SoS, this research only identifies the SoS top-level functions. The resulting top-level functions are reconnaissance, surveillance, and tracking. Following are the descriptions of the platforms and sensor used in a coalition MDA SoS.

1. Australian Platform/Sensors

a. AP-3C/W

The Royal Australian Air Force (RAAF) P-3C/W aircraft (Figure 1) is a modified version of the U.S. P-3 Orion maritime patrol aircraft. Manufactured by Lockheed, the P-3 aircraft is used by numerous militaries around the world for maritime

patrol, reconnaissance, surveillance, and anti-submarine warfare. All RAAF P-3C/W aircraft have been fully upgraded with systems by L-3 Communications to include an Elta Synthetic Aperture Radar/Inverse Synthetic Aperture Radar (SAR/ISAR) RADAR.

Figure 1. Australian AP-3C/W conducting maritime patrol. (From: [13].)

b. SAR/ISAR RADAR

Synthetic Aperture Radar (SAR) technology plays a key role in surveillance and reconnaissance missions by providing information for developing maritime domain awareness. SAR refers to a technique used to synthesize a very long antenna by combining signals (echos) received by the radar as it moves along its flight path. SAR systems constitute a very powerful tool for observation since they can acquire images independently of weather and solar illumination. SAR systems can image targets at extremely high resolutions and long ranges. SAR systems produce high-resolution images by using sophisticated post-processing of the radar data.

2. Canadian Platform/Sensors

a. Project Polar Epsilon

Project Polar Epsilon is a space-based wide area surveillance and support capability within Canada's Defence program. The primary sensor in project Polar Epsilon is Canada's RADARSAT-2 Earth Observation satellite (Figure 2). One of the main capabilities Polar Epsilon will deliver is near real-time ship detection, thereby helping create a maritime picture in support of MDA. Currently geared primarily for Canadian homeland protection, Project Polar Epsilon's RADARSAT-2 satellite may be deployed to cover other regions of the globe.

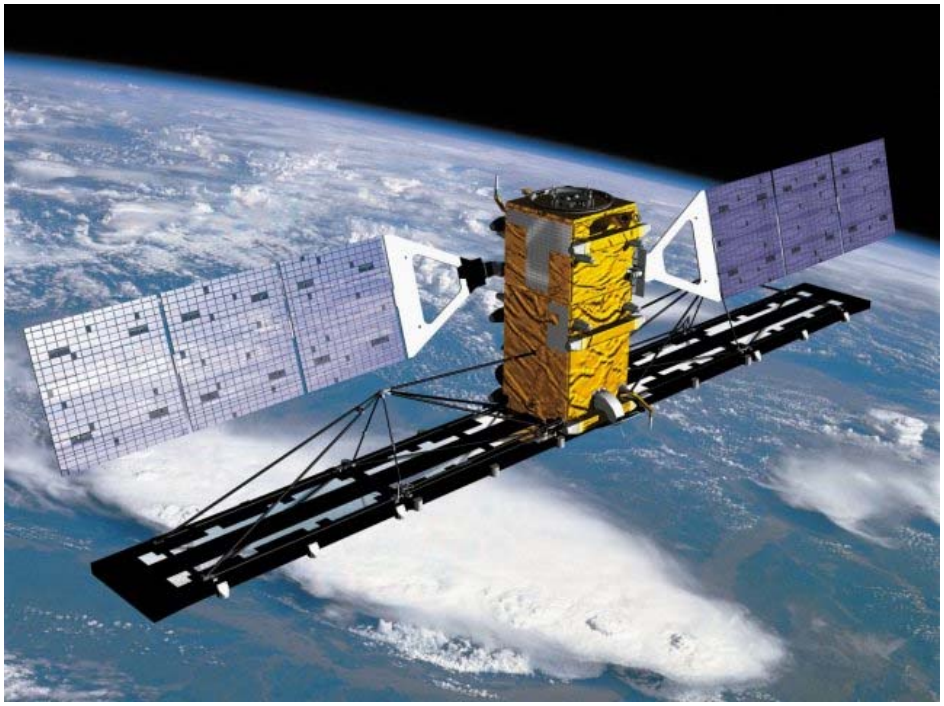

Figure 2. Artist rendition of Canada's RADARSAT-2 satellite. (From: [14].)

b. RADARTSAT-2

RADARSAT-2, a remote sensing satellite, uses state-of-the-art radar technology to provide the most advanced commercially available SAR imagery in the world [11]. Using SAR technology in a special ship-detection mode, RADARSAT-2 is

able to detect ships and small vessels in the ocean over large geographic areas. RADARSAT-2 will also detect uncooperative vessels regardless the absence of emissions in the EM spectrum [11]. Once the data is gathered and processed, the information can be used to cue other reconnaissance assets such as optical satellites, patrol aircraft, unmanned aerial vehicles (UAV), and ships.

3. United States Platform/Sensors

a. Global Hawk

The USAF RQ-4A (or USN RQ-4B) Global Hawk is a high-altitude (65,000 ft), long-endurance (42 hours) unmanned aerial reconnaissance system which provides commanders with high resolution, near real-time imagery of large geographic areas. The Global Hawk (Figure 3) can conduct reconnaissance missions in all types of operations. Having a 14,000 nautical mile range combined with satellite and line-of-sight communications, the Global Hawk can be deployed for operations world-wide, including maritime domain awareness.

Figure 3. USAF RQ-4A Global Hawk high-altitude, long-endurance unmanned aerial reconnaissance system. (From: [15].)

Remote sensing platforms, like air-based UAVs and space-based satellites, have many advantages and disadvantages. Global Hawk's main advantage when performing persistent surveillance is its long endurance and on-station time. Space-based assets may be able to fix a target's location at a particular point in time, but usually lack the ability to persistently track a target over time.

The Global Hawk's primary sensors are contained in the Integrated Sensor Suite (ISS), which includes synthetic aperture radar and electo-optical and infrared sensor systems. The Global Hawk's sophisticated electronics allow it to penetrate through the clouds during day or night operations. The SAR sensor has a Moving Target Indicator, which allows tracking small moving objects on the ground or ocean, and a powerful digital camera and infrared sensor, which allows gathering imagery in all weather conditions. After collecting reconnaissance data, the ISS sends the data to a ground station, which receives the high-quality imagery, and then forwards the imagery to military commanders in the field.

b. U. S. Ship—Bunker Hill Class Cruiser

The Bunker Hill class (old Ticonderoga class) guided missile cruisers are the U.S. Navy's only active cruisers and the first combatant warships to apply the increased combat capability of the Aegis combat system and the AN/SPY-1 phased-array radar system. Figure 4 shows one of the twenty-two cruisers in the U. S. Fleet.

Figure 4. USS Monterey (CG 61), one of twenty-two Bunker Hill class cruisers in the U.S. Navy. (From: [16].)

c. U.S. Ship—Arleigh Burke Class Destroyer

The Arleigh Burke class guided missile destroyers are the U.S. Navy's only active class of destroyers. Built around the Aegis combat system, the Arleigh Burke class is among the largest and most powerful destroyers ever built. Figure 5 shows one of the more than fifty Arleigh Burke class destroyers in the U.S. Fleet.

Figure 5. USS Pinkney (DDG 91), one of the U.S. Navy's Arleigh Burke class Flight II destroyers. (From: [17].)

The primary sensor on both the Bunker Hill and Arleigh Burke class ships is the AN/SPY-1D multi-function phased-array radar. The AN/SPY-1D radar is the key component of the Aegis combat system providing 360-degree coverage to track surface and air contacts.

4. External Sources

Some sources, such as the Intelligence Community, Automated Identification System, and various databases, are considered to be external to the MDA SoS.

a. Intelligence Community

The Intelligence Community (IC) is a federation of executive branch agencies and organizations that conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the U.S. [18]. The IC organizes and manages the collection of intelligence from various sources or disciplines. For example, an intelligence gathering discipline, which collects information via remote sensing satellite and aerial photography, is known as imagery intelligence. Other common intelligence gathering disciplines include signals intelligence and human intelligence.

b. Automatic Identification System

The Automatic Identification System (AIS) is a system used by ships in the shipping industry for locating and identifying vessels. The AIS provides a means for ships to electronically exchange ship data, such as identification, position, course, and speed, with other nearby ships and vessel traffic service (VTS) transponder stations. Since the AIS is only required for ships larger than 300 gross tons, smaller craft and non-cooperative vessels are not captured by the AIS system. Figure 6 is an illustration of an AIS system concept.

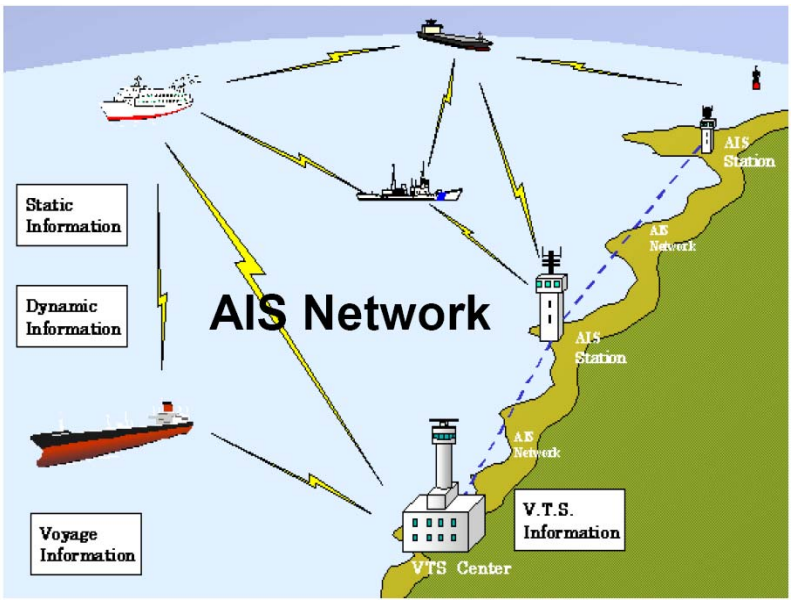

Figure 6. AIS Network depiction showing data exchange between ships and VTS stations. (From: [19].)

Originally intended for collision avoidance, the AIS, along with the VTS transponder system, is proving to be a valuable asset to identify ships in SAR imagery, especially as future space systems become capable of receiving and interpreting the AIS signals from space.

c. Commercial, Industry, and Open Source Databases

Various databases, both commercial and open source, contain a voluminous amount of information that could potentially aid in profiling and identifying PAVs and cargo. For example, cargo from a country known to harbor terrorists could raise a warning flag. Since ships are supposed to document their cargo contents, perhaps containers with odd routings or ships with suspicious manifests would raise a different warning flag. Among several commercial and open source databases that could provide invaluable information for maritime awareness, Lloyd's MIU offers services that track vessel movement data, and provides AIS movements, casualty and characteristics data, as well as a huge database of 163,500 shipping companies [20].

E. SUMMARY

This chapter defines maritime domain awareness, discusses the net-centric operations concept, and explains multi-domain system of systems. It then defines the multi-domain awareness problem statement and scenario. Finally, it describes the assets available to contribute to an MDA SoS. The next chapter provides an overview of the integrated systems engineering methodology employed in this research, as well as brief descriptions and the interrelations between the SoS Architecture Development Process, DoDAF products, and SysML diagrams.

THIS PAGE INTENTIONALLY LEFT BLANK

III. INTEGRATED SYSTEMS ENGINEERING METHODOLOGY

A. INTRODUCTION

The integrated systems engineering methodology for performing engineering analyses of systems of systems, developed at the Naval Postgraduate School [3], [21], [22], has been successfully applied to example military systems of systems [3], [23]. The integrated systems engineering methodology applies to systems of systems formed by systems that have previously been independently developed as stand-alone systems. An elaboration of the integrated systems engineering methodology follows.

1. SoS Systems Engineering

Systems of systems engineering is the design, development, and operation of a system of stand-alone systems that provides functions the stand-alone systems cannot provide [24]. Many existing systems alone can be considered complex systems. However, future demands require these systems be engineered to function as an integrated system of systems (SoS). An SoS is defined as "a conglomeration of existing, stand-alone systems or to-be-defined and to-be-evaluated systems that are integrated and interoperable with each other" [3]. Two systems are interoperable if they can successfully exchange and process information in support of a task or mission.

2. Systems Engineering Methodology for Analyzing SoS

An SoS systems engineering problem involves analysis of existing and proposed systems of systems architectures as well as of architectures of complex systems-of-systems [22], [23]. Processes are a series of actions undertaken to produce products, services, or other end results used by systems. The integrated systems engineering methodology is a process modeling methodology for performing engineering analysis for systems of systems [21]. The methodology was first developed using the unified modeling language (UML) for systems modeling. It then used the systems modeling language (SysML) to take advantage of the features offered by SysML [3], [25], [26].

3. Integrated Systems Engineering Methodology

The integrated systems engineering methodology is an integrated methodology for analyzing SoS architectures, using modeling and simulation, and provides traceability between executable models and the SoS architecture. The methodology unites and integrates three parts into a unified paradigm for analysis of SoS architectures. The three parts of the integrated systems engineering methodology are [3], [23]:

- SoS Architecture Development Process (SoSADP);
- Department of Defense (DoD) Architecture Framework (DoDAF); and
- SysML.

The SoSADP[2] is a framework for assessing SoS architectures using modeling and simulation. A logical, systemic, layered process, the SoSADP starts with the needs for a SoS and ends with SoS architectures assessed and ranked using modeling and simulation. The DoDAF defines a common approach for DoD architectural description development, presentation, and integration [27], [28]. The integrated systems engineering methodology integrates the SoSADP with the development of the DoDAF products and SysML diagrams in representing an SoS architecture.

The SoSADP is further explained in Section B, followed by the DoDAF and DoDAF products in Section C, SysML in Section D, and finally, the unified paradigm or mapping in Section E.

B. SYSTEM OF SYSTEMS ARCHITECTURE DEVELOPMENT PROCESS

This section is excerpted from Huynh and Osmundson [3]. The first part of the SoS systems engineering methodology is the SoSADP. A logical, layered process, the SoSADP provides a framework for assessing SoS architectures. Figure 7 captures the SoSADP with the processes within a layer supporting the processes in the layer immediately above. The connectors in red depict the support relationships—from a lower layer to an upper layer—while those in blue show the local (within a layer) relationships.

[2] Developed by Dr. Thomas Huynh while at Lockheed Martin (circa 2001), the SoSADP has been adopted and modified for use in the Systems Engineering Department for projects at NPS.

The SoSADP starts with the SoS problem and ends with ranked SoS architectures. As with any systems engineering process, the iterative nature is also inherent in the SoSADP. Each SoSADP layer is described in greater detail below.

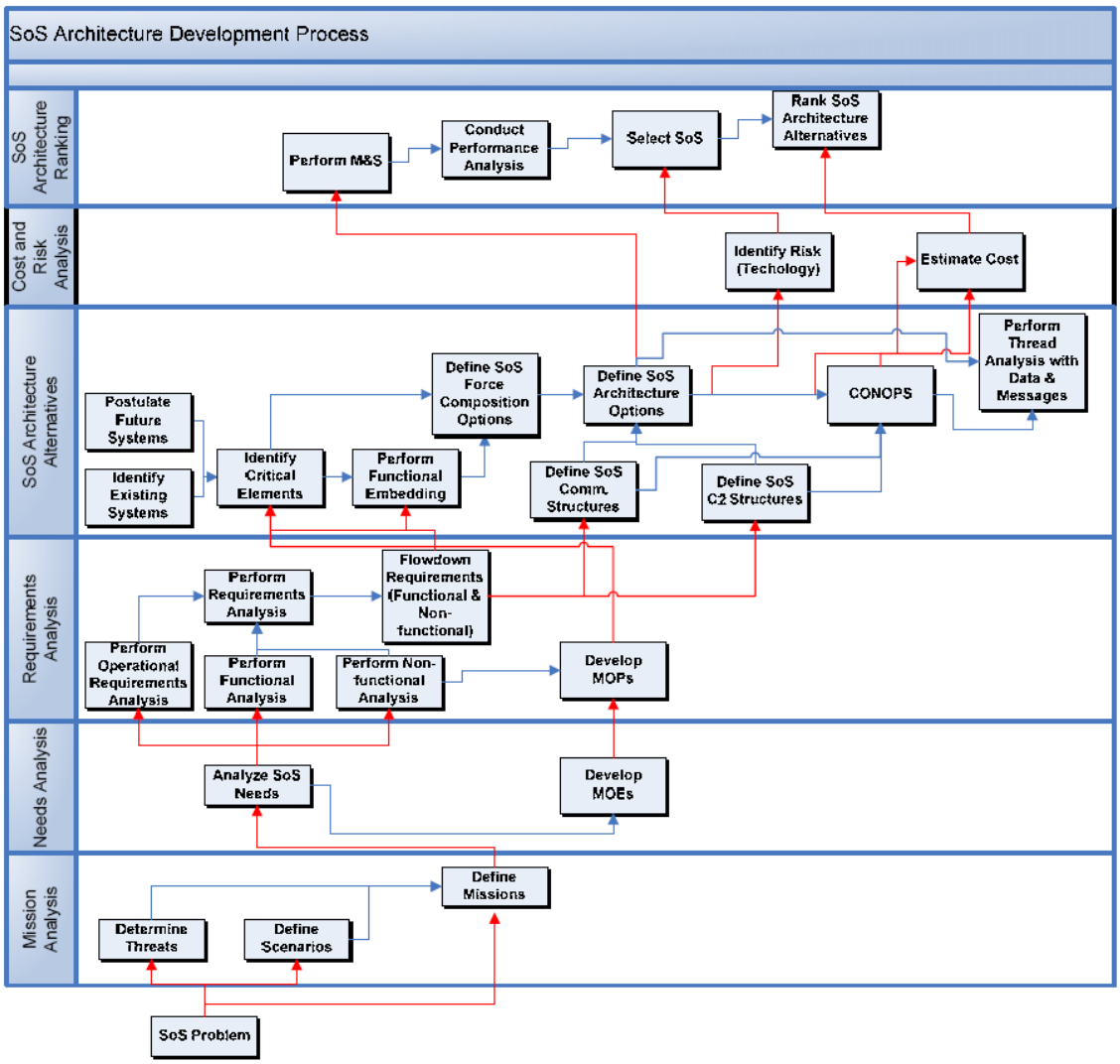

Figure 7. The layered structure of the SoS architecture development process (SoSADP) (From: [3].)

1. SoS Problem

The SoS problem statement is a description of the SoS that needs to be built and sets in motion the SoSADP. The SoS problem statement provides missions, threats, unilateral or coalition undertakings, timeframes, geographical settings, needs for an SoS, and constraints.

2. Mission Analysis

Mission analysis consists of determining the threats (*Determine Threats*[3]), defining scenarios (*Define Scenarios*), and refining the missions (*Determine Missions*). A scenario includes the threats, their signatures, their trajectories, etc., the deployment of the defense forces, and the physical environment in which the mission takes place or is executed.

3. Needs Analysis

The needs analysis layer is built upon the output of the *Define Missions* in the Missions Analysis layer. *Analyze SoS Needs* ascertains what functions the SoS must perform to execute the mission(s). *Develop MOEs* (measures of effectiveness) establishes how well the SoS must do to support the mission(s).

4. Requirements Analysis

The requirements analysis layer is built upon the output from the needs analysis layer. *Perform Requirements Analysis* is realized by *Perform Operational Requirements Analysis*, *Perform Functional Analysis*, and *Perform Non-functional Analysis*, all of which use the output from *Analyze SoS Needs*. *Perform Operational Requirements Analysis* provides operational requirements. *Perform Functional Analysis* results in a functional description of the SoS and all facets of SoS operations and support and is accomplished through functional decomposition and allocation and development of functional flow diagrams. *Perform Non-functional Analysis* provides quantitative requirements. *Flowdown Requirements* is then performed using the results from *Perform Requirements Analysis*. Finally, *Develop MOPs* (measures of performance) uses the output from the *Develop MOEs*.

[3] Italicized phrases in this section denote processes.

5. SoS Architecture Alternatives

The requirements analysis layer supports the SoS Architecture Alternatives layer. *Identify Critical Elements*, *Perform Functional Embedding*, *Define SoS Communications Structures*, and *Define SoS C2* (command and control) *Structures* use the output from *Flowdown Requirements* and *Develop MOPs* from the layer immediately below. *Perform Functional Embedding* allocates functions to systems that make up the SoS. *Identify Critical Elements* establishes critical elements of the desired SoS. *Identify Existing Systems* identifies current systems with the required capabilities. *Postulate Future Systems* proposes future system elements. The results of *Define SoS Communications Structures*, *Define SoS C2 Structures*, and *Define SoS Architecture Options* aid in the definition of the concept of operations (CONOPS) in *Define CONOPS*. *Define SoS Communication Structures* establishes different communication structures. *Define SoS C2 Structures* establishes different command and control structures. *SoS Force Composition Options* uses system elements and outputs of *Perform Functional Analysis* to define various for composition options. *Define SoS Architecture Options* generates SoS architectures using outputs from *SoS Force Composition*, *Define SoS Communication Structures*, and *Define SoS C2 Structures*. *Develop Threads with Data & Messages* uses the results from *Define SoS Architecture Options* and *Define CONOPS*.

6. Cost and Risk Analysis

The SoS architecture alternatives layer supports the cost and risk analysis layer. *Estimate Cost* and *Identify Risks* provide the total cost and the risks associated with the different SoS architecture alternatives.

7. SoS Architecture Ranking

Perform M&S (modeling and simulation) models the SoS used in simulation to aid *Conduct Performance Analysis* in assessing the performance of the SoS architecture alternatives. *Select SoS* selects the best SoS architecture. *Rank SoS Architecture Alternatives* ranks the SoS architecture alternatives, using the estimated MOPs and MOEs, costs, and risk factors.

C. DEPARTMENT OF DEFENSE ARCHITECTURE FRAMEWORK

The second part of the SoS systems engineering methodology is the DoDAF and its products. This section starts by briefly describing the difference between architecture and an architecture framework. It is important to understand the difference before describing the specifics of the DoDAF. This is followed by an overview of the DoDAF, specifically its purpose, views, and products.

1. Architectures and Architecture Frameworks

According to IEEE STD 1471-2000,[4] architecture is defined as "the fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution" [29]. Architecture represents or describes a defined domain, at a current or future point in time, in terms of building blocks, how those blocks function, the rules and constraints under which those blocks function, and how those blocks relate to each other and to the environment [28]. An architecture framework, on the other hand, provides guidance and rules for structuring, classifying, and organizing architectures. An architecture framework is a tool that describes a method for designing a system in terms of a set of building blocks, showing how the building blocks fit together. An architecture framework provides a common vocabulary and a list of recommended standards and compliant products that can be used to implement the building blocks [28]. The DoDAF, for example, provides the U.S. defense industry a foundation or guidance to ensure system standards and interoperability.

The architecture framework (Figure 8) consists of two layers: data and presentation. The data layer contains the architecture data elements and their defining attributes and relationships. The presentation layer contains the products and views that support a visual means to communicate and understand the purpose of the architecture, what it describes, and the various architectural analyses performed. Products provide a

[4] Institute for Electrical and Electronics Engineers (IEEE) is one of the leading standards-making organizations in the world. IEEE STD 1471-2000 is the Recommended Practice for Architecture Description of Software-Intensive Systems.

way for visualizing architecture data as graphical, tabular, or textual representations. Views provide the ability to visualize architecture data that stem across products, logically organizing the data for a specific or holistic perspective of the architecture [28].

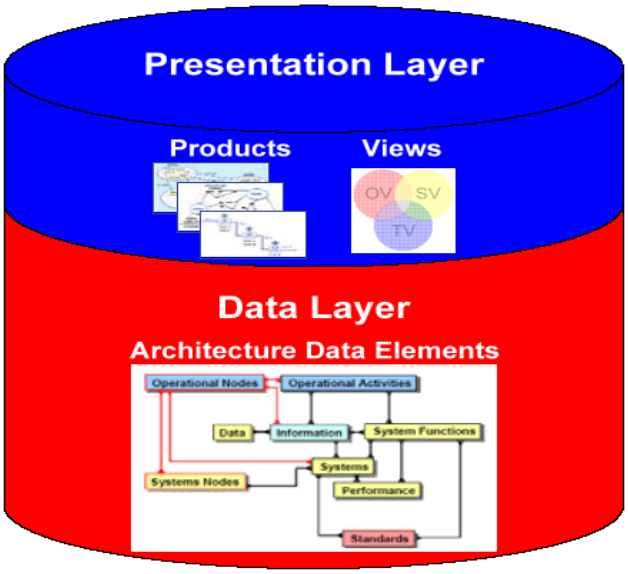

Figure 8. Architecture Framework Structure (From: [4].)

2. DoDAF Purpose

The purpose of the DoDAF is to provide guidance for describing DoD architectures for both warfighting and business operations and processes. DoDAF defines a common approach for DoD architectural description development, presentation, and integration; thus establishing a common denominator for understanding, comparing, and integrating architectures across organizational, Joint, and multinational boundaries. DoDAF version 1.5, responding to the DoD's migration towards NCO, applies net-centric concepts by placing more emphasis on architecture data to facilitate more efficient and flexible use and reuse of architecture data, enabling broader utility for decision makers and process owners [30].

3. DoDAF Views

The DoDAF provides an integrated architecture with data elements that are uniquely identified and consistently used across all products and views within the architecture. In most cases, an integrated architecture description has an Operational View (OV), Systems and Services View (SV), Technical Standards View (TV), and an All View (AV) that are integrated with each other. Figure 9 represents the information that links the operational view, systems and services view, and technical standards view, also showing there are common points of reference linking the OV and SV and also linking the SV and TV. The following definitions of OV, SV, TV, and AV are excerpted from the DoDAF v1.5.

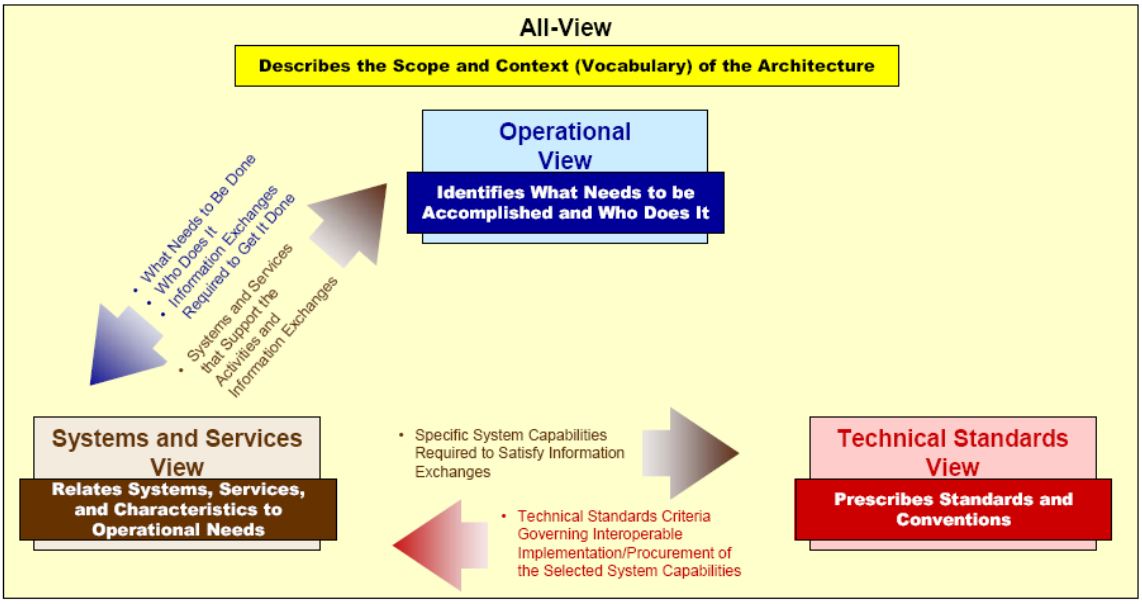

Figure 9. Fundamental Linkages among Views. (From: [4].)

a. Definition of the Operational View (OV)

The Operational View captures the operational nodes, the tasks or activities performed, and the information that must be exchanged to accomplish DoD missions. The OV conveys the types of information exchanged, the frequency of exchange, which tasks and activities are supported by the information exchanges, and the nature of information exchanges [28].

b. Definition of the Systems and Services View (SV)

The Systems and Services View captures system, service, and interconnection functionality providing for, or supporting, operational activities. DoD processes include warfighting, business, intelligence, and infrastructure functions. The SV system functions and service resources and components may be linked to the architecture artifacts in the OV. These system functions and service resources support the operational activities and facilitate the exchange of information among operational nodes [28].

c. Definition of Technical Standards View (TV)

The Technical Standards View is the set of rules governing the arrangement, interaction, and interdependence of system parts or elements. The TV's purpose is to ensure that a system satisfies a specified set of operational requirements. The TV provides the technical systems implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed. It includes a collection of the technical standards, implementation conventions, standards options, rules, and criteria that can be organized into profiles(s) that govern systems and system or service elements for a given architecture [28].

d. Definition of All View (AV)

The All View relates some overarching aspects of an architecture that may cross all three views. These overarching aspects are captured in the AV products. The AV products provide information pertinent to the entire architecture but do not represent a distinct view of the architecture. AV products set the scope and context of the architecture. The scope includes the subject area and time frame for the architecture. The setting in which the architecture exists comprises the interrelated conditions that compose the context for the architecture. These conditions include doctrine; tactics, techniques, and procedures; relevant goals and vision statements; concepts of operation (CONOPS); scenarios; and environmental conditions [28].

4. DoDAF Products

The DoDAF products describe characteristics pertinent to the architecture purpose through graphical, textual, and tabular forms. Each view consists of architecture products, which are interrelated within a view as well as across views. Table 1 lists the architecture products for each view, as defined in DoDAF v1.5.

Table 1. DoDAF List of Products. (From: [4].)

Applicable View	Framework Product	Framework Product Name	Net-Centric Extension	General Description
All View	AV-1	Overview and Summary Information	✓	Scope, purpose, intended users, environment depicted, analytical findings
All View	AV-2	Integrated Dictionary	✓	Architecture data repository with definitions of all terms used in all products
Operational	OV-1	High-Level Operational Concept Graphic	✓	High-level graphical/textual description of operational concept
Operational	OV-2	Operational Node Connectivity Description	✓	Operational nodes, connectivity, and information exchange need lines between nodes
Operational	OV-3	Operational Information Exchange Matrix	✓	Information exchanged between nodes and the relevant attributes of that exchange
Operational	OV-4	Organizational Relationships Chart	✓	Organizational, role, or other relationships among organizations
Operational	OV-5	Operational Activity Model	✓	Capabilities, operational activities, relationships among activities, inputs, and outputs; overlays can show cost, performing nodes, or other pertinent information
Operational	OV-6a	Operational Rules Model	✓	One of three products used to describe operational activity—identifies business rules that constrain operation
Operational	OV-6b	Operational State Transition Description	✓	One of three products used to describe operational activity—identifies business process responses to events
Operational	OV-6c	Operational Event-Trace Description	✓	One of three products used to describe operational activity—traces actions in a scenario or sequence of events
Operational	OV-7	Logical Data Model	✓	Documentation of the system data requirements and structural business process rules of the Operational View
Systems and Services	SV-1	Systems Interface Description Services Interface Description	✓	Identification of systems nodes, systems, system items, services, and service items and their interconnections, within and between nodes
Systems and Services	SV-2	Systems Communications Description Services Communications Description	✓	Systems nodes, systems, system items, services, and service items and their related communications lay-downs
Systems and Services	SV-3	Systems-Systems Matrix Services-Systems Matrix Services-Services Matrix	✓	Relationships among systems and services in a given architecture; can be designed to show relationships of interest, e.g., system-type interfaces, planned vs. existing interfaces, etc.
Systems and Services	SV-4a	Systems Functionality Description		Functions performed by systems and the system data flows among system functions
Systems and Services	SV-4b	Services Functionality Description	✓	Functions performed by services and the service data flow among service functions
Systems and Services	SV-5a	Operational Activity to Systems Function Traceability Matrix		Mapping of system functions back to operational activities
Systems and Services	SV-5b	Operational Activity to Systems Traceability Matrix		Mapping of systems back to capabilities or operational activities
Systems and Services	SV-5c	Operational Activity to Services Traceability Matrix	✓	Mapping of services back to operational activities
Systems and Services	SV-6	Systems Data Exchange Matrix Services Data Exchange Matrix	✓	Provides details of system or service data elements being exchanged between systems or services and the attributes of that exchange

Applicable View	Framework Product	Framework Product Name	Net-Centric Extension	General Description
Systems and Services	SV-7	Systems Performance Parameters Matrix Services Performance Parameters Matrix	✓	Performance characteristics of Systems and Services View elements for the appropriate time frame(s)
Systems and Services	SV-8	Systems Evolution Description Services Evolution Description	✓	Planned incremental steps toward migrating a suite of systems or services to a more efficient suite, or toward evolving a current system to a future implementation
Systems and Services	SV-9	Systems Technology Forecast Services Technology Forecast	✓	Emerging technologies and software/hardware products that are expected to be available in a given set of time frames and that will affect future development of the architecture
Systems and Services	SV-10a	Systems Rules Model Services Rules Model	✓	One of three products used to describe system and service functionality—identifies constraints that are imposed on systems/services functionality due to some aspect of systems design or implementation
Systems and Services	SV-10b	Systems State Transition Description Services State Transition Description	✓	One of three products used to describe system and service functionality—identifies responses of a system/service to events
Systems and Services	SV-10c	Systems Event-Trace Description Services Event-Trace Description	✓	One of three products used to describe system or service functionality—identifies system/service-specific refinements of critical sequences of events described in the Operational View
Systems and Services	SV-11	Physical Schema	✓	Physical implementation of the Logical Data Model entities, e.g., message formats, file structures, physical schema
Technical Standards	TV-1	Technical Standards Profile	✓	Listing of standards that apply to Systems and Services View elements in a given architecture
Technical Standards	TV-2	Technical Standards Forecast		Description of emerging standards and potential impact on current Systems and Services View elements, within a set of time frames

The first column indicates the view applicable to each product. The second column provides an alphanumeric reference identifier for each product. The third column gives the formal name of the product. The fourth column indicates if the product's definition and purpose are augmented to incorporate net-centric concepts. The fifth column captures the general nature of the product's content. The sequence of products in the table does not imply a sequence for developing the products. However, an implied support structure does exist among the products, albeit developed iteratively, which captures the views and the products in a layered construct depicted in Figure 10 [3]. Again, the lower layer supports the layer immediately above it. The AV supports the OV, which supports the SV, which supports the TV. The arrows in red indicate the connections between layers. The arrows in other colors are local to the layers to which they belong.

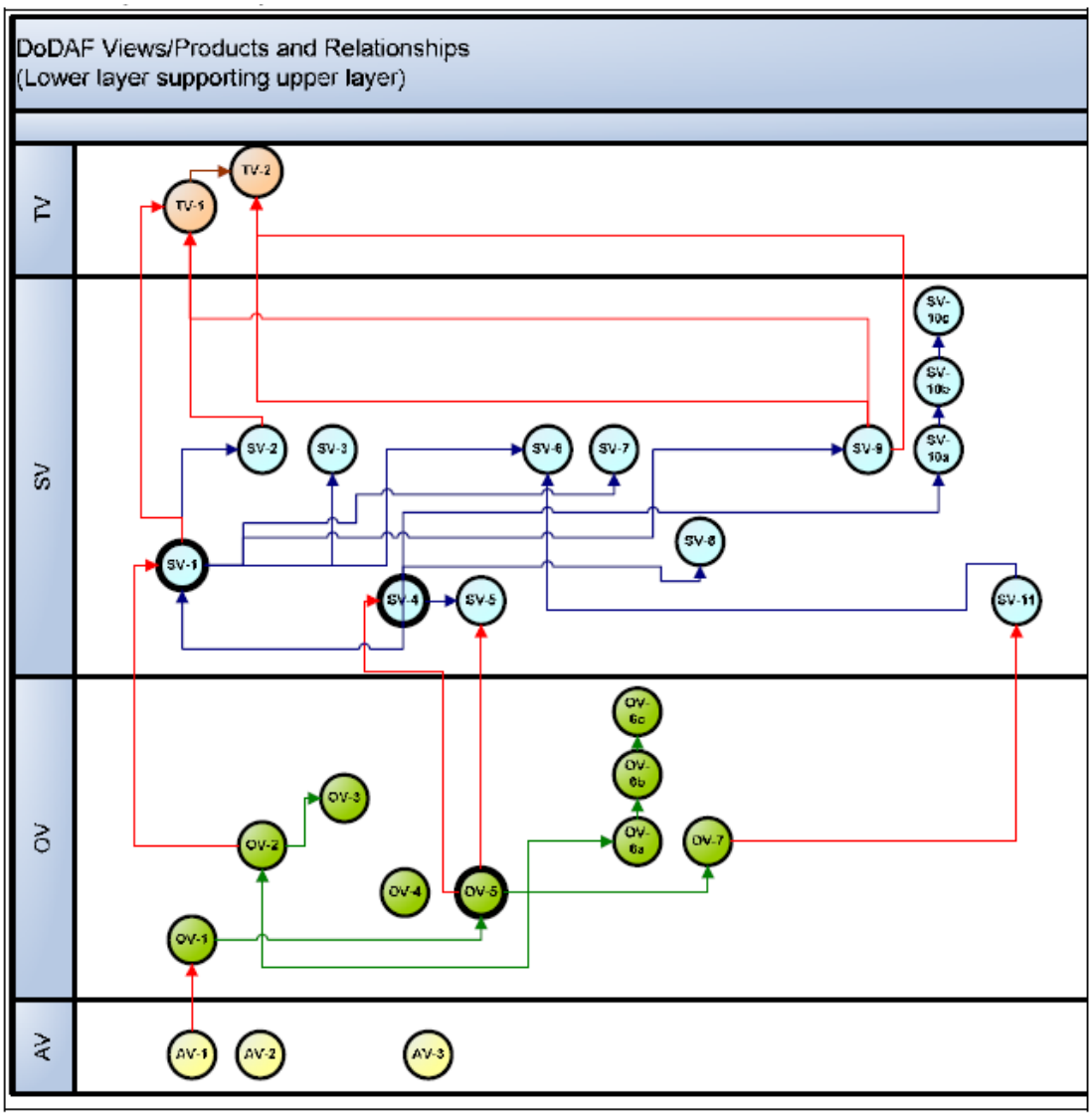

Figure 10. The layered structure depicting the interrelations among the DoDAF views and their associated architecture products. (From: [3].)

This thesis is confined to a multi-domain awareness SoS architecture that is integrated and NCOW-compliant. An integrated, NCOW-compliant SoS architecture requires twelve DoDAF products, at a minimum [27]: AV-1, AV-2, OV-2, OV-3, OV-5, SV-1, TV-1, together with the products required by NCOW, OV-1, SV-2, SV-3, SV-4, and SV-5.

D. SYSTEMS MODELING LANGUAGE (SYSML)

1. SysML Introduction

Systems Modeling Language (SysML) is a general-purpose graphical modeling language for specifying, analyzing, designing, and verifying all types of complex systems. SysML uses graphical representations, which are effective in specifying system requirements, system structure, functional behavior, and parametrics during the specification and design phases of a systems engineering problem. SysML is designed to provide simple yet powerful models that aid in solving a variety of systems engineering problems.

SysML is defined as an extension of a subset of the Unified Modeling Language (UML). SysML reuses a subset of UML and provides additional extensions needed to satisfy the requirements in UML for the systems engineering domain. The Venn diagram (Figure 11) shows the visual relationship between the UML and SysML languages, where the large circles represent the set of language constructs that comprise UML and SysML, respectively. The intersection of the two circles, shown in the shaded region, indicates the UML modeling constructs that SysML reuses [5].

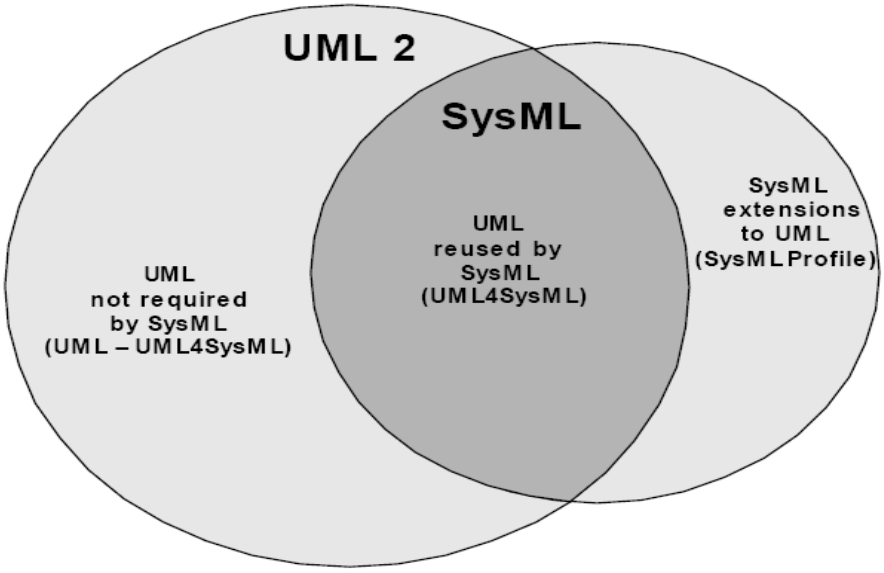

Figure 11. Overview of SysML/UML interrelationship. (From: [5].)

There are advantages that may be gained by using SysML over UML when modeling systems. SysML can be used for representing systems and product architectures, as well as their behavior and functionality. For example, the SysML Requirements diagrams efficiently capture a system's functional, performance, and interface requirements; however, there are limitations to define high-level functional requirements using UML Use Case diagrams. Also, SysML Parametric diagrams are used to define performance and mechanical constraints, but UML does not provide any direct mechanism to capture essential performance and mechanical information.

2. SysML Diagrams

SysML uses a variety of diagrams with a semantic foundation to represent complex systems. SysML modifies some existing UML constructs and adds specialized constructs to address unique systems engineering requirements. Figure 12 shows an example of the SysML diagram taxonomy. A diagram taxonomy makes it easier to visualize how SysML reuses or modifies many of the existing UML diagram types, and adds new diagram types when additional requirements or constructs arise.

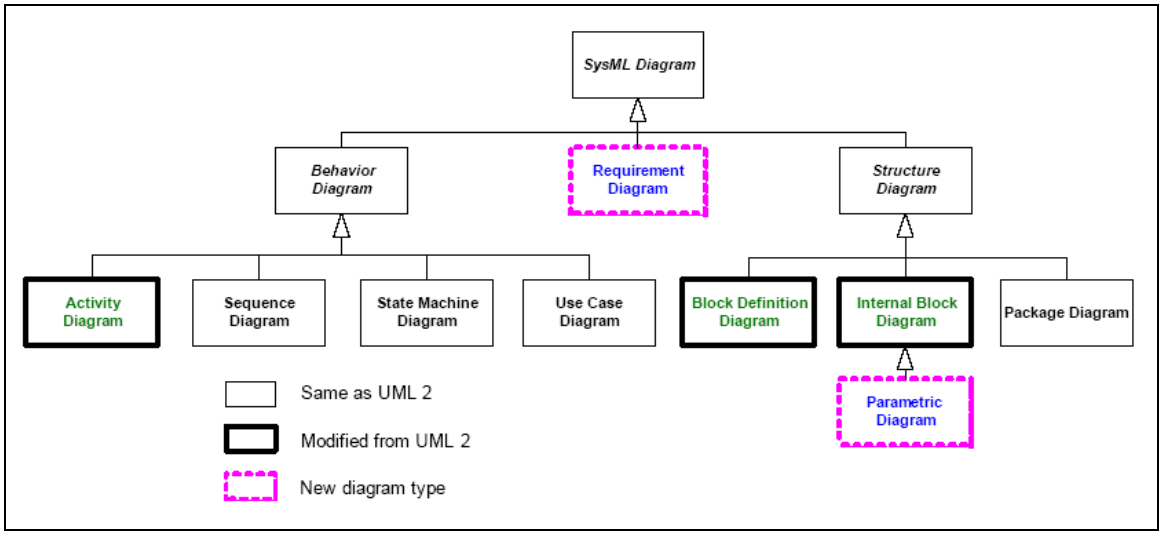

Figure 12. SysML Diagram Taxonomy. (From: [5].)

A SysML diagram represents a model element and has a diagram frame with a header. The header displays diagram kind, model element type, model element name, and

descriptive diagram name or view name. A diagram kind can be labeled ‘act’ for activity, ‘bdd’ for block definition diagram, ‘ibd’ for internal block diagram, etc. A model element type includes activity, block, interaction, etc. Figure 13 shows an example SysML diagram.

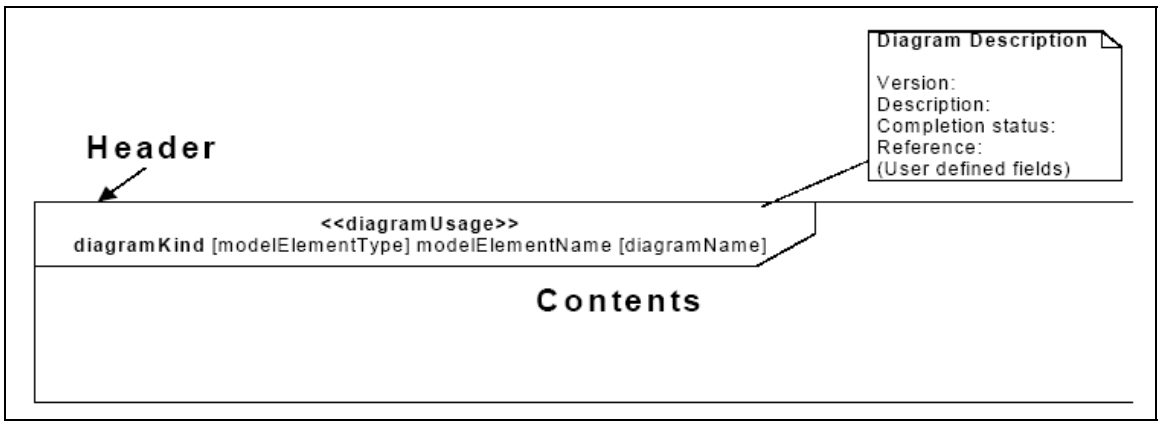

Figure 13. SysML diagram frame. (From: [5].)

The following six SysML diagram types are briefly defined. They are later used in this thesis to represent the SoS architecture. Their descriptions come from to the OMG Systems Modeling Language (OMG SysML) specification [5]. For more information concerning the SysML diagrams or SysML in general, refer to the OMG SysML specification.

a. Context Diagram

The context diagram is simple in nature, yet it is one of the most important diagrams when modeling a system. One of the most important tasks surrounding a systems engineering problem is to decide what belongs to the system and what is external to the system. The context diagram is an informal way to represent the boundaries of the system.

b. Use Case Diagram

The use case diagram describes the usage of a system by its environment to achieve a goal. The environment includes actors, which the system may be providing

services to or getting services from that are external to the system. The use case can also show the functionality and/or capabilities of the system through the interactions between the system and its actors, including communications that may occur among them.

c. Requirements Diagram

The requirements diagram displays requirements, packages, other classifiers, test cases, and rationale. The requirement specifies a capability or condition that must be met or satisfied. It can depict the requirements in graphical, tabular, or tree structure format. This diagram is one of the modeling constructs intended to provide a bridge between traditional requirements management tools and other SysML models [5].

d. Activity Diagram

The activity diagram graphically models the inputs, outputs, sequences, and conditions for coordinating other behaviors. Activity diagrams provide a flexible link to the blocks owning those behaviors.

e. Sequence Diagram

The sequence diagram describes the flow of control between actors and parts of the system. It also represents both communication and timing among entities, where time is represented on the vertical axis. For example, the interactions could represent the sending and receiving of messages between interacting entities.

f. Block Definition (Breakdown) Diagram

The block breakdown diagram in SysML defines features of blocks and relationships between blocks such as associations, generalizations, and dependencies. It defines a decomposition of the activities and object flows from an activity diagram.

E. INTERRELATIONS BETWEEN SOSADP, DODAF PRODUCTS, AND SYSML DIAGRAMS

The mapping between the SoSADP, DoDAF products development, and SysML diagrams development (Figure 14) underlies the scope of the integrated methodology used in this research [21]. The SoSADP remains the starting point of the integrated methodology. A layer-to-layer mapping allows the DoDAF products in the DoDAF layers to capture the results from the SoSADP processes. The SysML diagrams in the four pillars of SysML—namely, Structure, Behavior, Requirements, and Parametrics—capture the results of the SoSADP processes [3]. The mapping between the SoSADP processes and the SysML diagrams are not necessarily one-to-one.

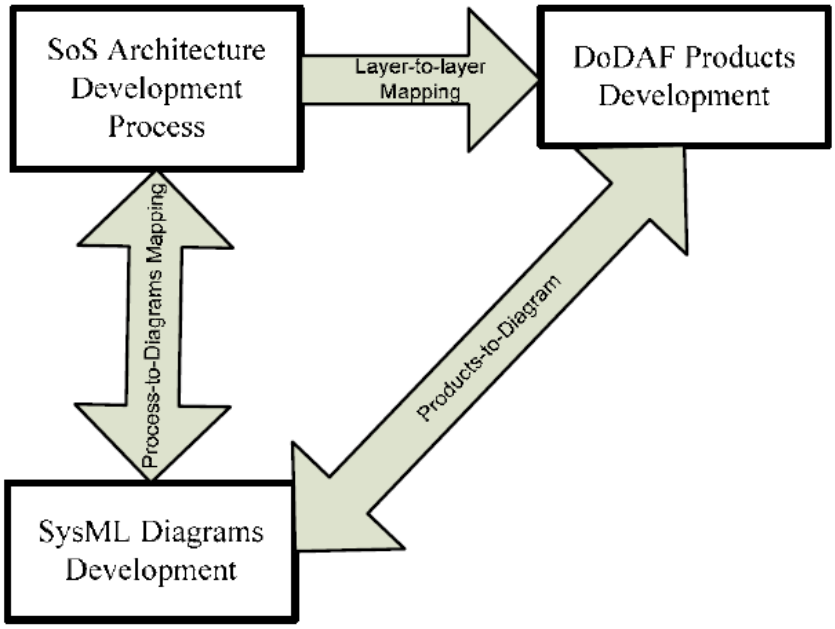

Figure 14. The mapping between the SoSADP, DoDAF products, and SysML diagrams development. (From: [3].)

Table 2 displays the various DoDAF products for an integrated, NCOW-compliant SoS architecture that capture some of the results from the SoSADP and the SysML diagrams that represent the DoDAF products and the SoSADP results. The SysML diagrams explicitly depict an SoS architecture graphically and aid in the

verification of the traceability between an SoS architecture and an executable model that represents the SoS architecture. Note that a blank space in Table 2 implies that there is no mapping among the entities of the SoSADP, DoDAF products, and SysML.

Table 2. The mapping between the SoSADP, DoDAF, and SysML diagrams for an integrated, NCOW architecture. (From: [3].)

SoSADP	DoDAF Product	SysML Diagrams							
		Requiremen	Structure		Behavior			EngrAnalysis (Performance)	
		Requirement Diagram	Block Diagram	Parametric Diagram	Activity Diagram	Sequence Diagram	Use Cases	Modeling & Simulation	Context Diagram
SoS Problem	Textual information (not AV-1)								
Needs Analysis									
Analyze SoS Needs	Textual information (part of AV-1)								
Develop MOEs				√					
Mission Analysis	**AV-1, OV-1**								
Determine Threats	OV-1 (High-level Operational Concept Graphic) AV-1 (Overview and Summary Information)						√		
Define Scenarios							√		√
Define Missions							√		√
Requirements Analysis	**OV-6, OV-5, SV-4, SV-5**								
Perform Operational Requirements Analysis	SV-4 (Systems Functionality Description)	√							
Perform Functional Analysis	SV-4 (Systems Functionality Description)	√							
Perform Non-functional Analysis		√							
Flowdown Requirements	SV-4 (Systems Functionality Description)	√						√	
Develop MOPs									
Perform Thread Analysis with Data & Messages	OV-6c (Operational Event Trace Description)				√	√			
SoS Architecture Alternatives	**OV-3**								
Define SoS Force Composition Options			√						√
Identify Critical Elements									
Identify Existing Systems									
Postulate Future Systems									
Perform Functional Embedding	SV-1 (Systems Interface)								
Define SoS Comm Structures			√						√
Define SoS C2 Structures	OV-4 (Organizational Relationships Chart)		√						√
Define SoS Architecture Options	SV-1 (Systems Interface)		√						√
Define CONOPS									
Develop concepts of operations	OV-5 (Operational Activity Model)				√	√			
Develop Internal Threads with Data & Messages	SV-1 (Systems Interface)				√	√			
Cost and Risk Analysis									
Model Cost									
Identify Risk									
SoS Architecture Ranking									
Perform M&S				√				√	
Conduct Performance Analysis				√				√	
Select SoS				√				√	
Rank SoS Architecture Alternatives				√				√	

F. SUMMARY

This chapter discusses the integrated systems engineering methodology for analyzing systems of systems. The integrated systems engineering methodology integrates the SoSADP, DoDAF products development, and SysML diagrams development into a unified paradigm for analysis of SoS architectures. Each of the

methodology's three components is described and examined in detail. The chapter concludes with a description of their interrelations and mapping between the SoSADP, DoDAF products, and SysML diagrams that will be used in the next chapter to produce representations of the SoS architecture alternatives.

IV. NCO MULTI-DOMAIN SOS ARCHITECTURE

A. INTRODUCTION

Maritime domain awareness is an area of strong interest to the U.S. and its allies. This chapter applies the integrated systems engineering methodology to the design and assessment of conceptual coalition multi-domain awareness SoS architectures. Again, a multi-domain SoS provides open-ocean reconnaissance and surveillance to create a maritime domain COP to aid in decision making. Furthermore, this research simplifies the DoDAF products and sketches SysML diagrams pertaining to the assessment of the multi-domain awareness SoS architectures by modeling and simulation.

B. MULTI-DOMAIN AWARENESS SYSTEM OF SYSTEMS

The coalition multi-domain awareness SoS problem stated in Chapter II may be simplified as follows: *architect an SoS consisting of capabilities, platforms, and sensors from coalition systems that will detect, track, and counter PAVs that potentially carry WMD in open-ocean transit, before reaching their seaports of destination. The multi-domain SoS consists of current or future coalition systems. The coalition nations available for this research are the U.S., Australia, and Canada*.

The scope of this thesis is limited to the scenario defined in Chapter II. Intelligence information on suspicious container ships, along with their locations, is received by the Coalition Command and Control center (CC2C). Requests for information from various external sources, such as AIS, shipping companies, and weather, are sent and received via the coalition network. The CC2C issues orders (with initial threat data) to the coalition nation command and control (C2) centers via the coalition network to track and monitor MV Alpha as a PAV. The Australian C2 center communicates with its platforms and sensors via the Australian network, the United States C2 center communicates with its platforms and sensors via the United States network, and the Canadian C2 center communicates with its platforms and sensors via the Canadian network. Each C2 center uses its distributed sensors (national, organic, and

commercial) to monitor and track MV Alpha as a PAV. All data collected by the distributed sensors networks from each coalition nation is processed, formatted, and sent via the coalition network to the CC2C to be integrated and fused into a COP. The COP is then disseminated to each coalition nation C2 center, thus providing a common picture of shared operational information facilitating MDA.

This research focuses only on the above portion of the scenario, while employing the operational view captured in Figure 15. This chapter discusses the application of the integrated systems engineering methodology to the analysis of a U.S.-Australia-Canada coalition multi-domain SoS architecture.

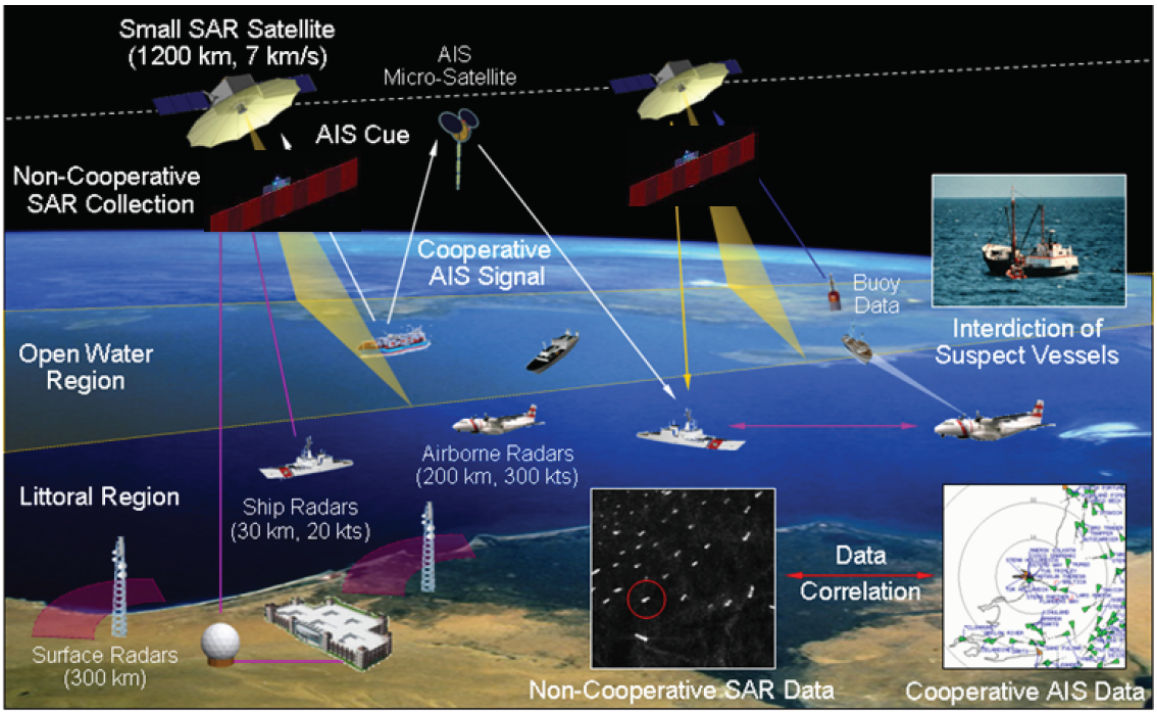

Figure 15. OV-1: The high-level operational concept of the coalition SoS. (From: [31].)

The OV-1 product (Figure 15), the high-level operational concept of the coalition SoS, depicts a network of a Coalition C2 center located on land (Guam or Hawaii), an Australian C2 center located in Darwin, Australia, a Canadian C2 center located in Vancouver, the U.S. C2 center located on one of the U.S. ships, and the coalition platforms and their respective sensors (as described in Chapter II). The Australian

network connects the Australian C2 center with the Australian sensors. The Canadian network connects the Canadian C2 center with the Canadian sensors. The U.S. sensors and C2 center communicate via the U.S. C2 network.

1. Context Diagram

The context diagram (Figure 16) sets the context and boundaries for the multi-domain awareness SoS. The context diagram depicts the top-level systems of the SoS. The <<system>> and <<external>> stereotypes help identify the multi-domain awareness SoS relative to its environment. The <<external>> elements, IntelInterface, ships (PAVs), ShipCompanies, Weather, and AISInterface, are considered to be external to the CoalitionMDASoS. The links, labeled X1 through X5, represent a connection between the CoalitionMDASoS and each <<external>> element. The connection may represent some type of an interaction such as data exchange or surveillance. In the multi-domain awareness SoS context diagram, the only connection that does not represent data exchange is X2, which represents an interaction of surveillance and/or tracking.

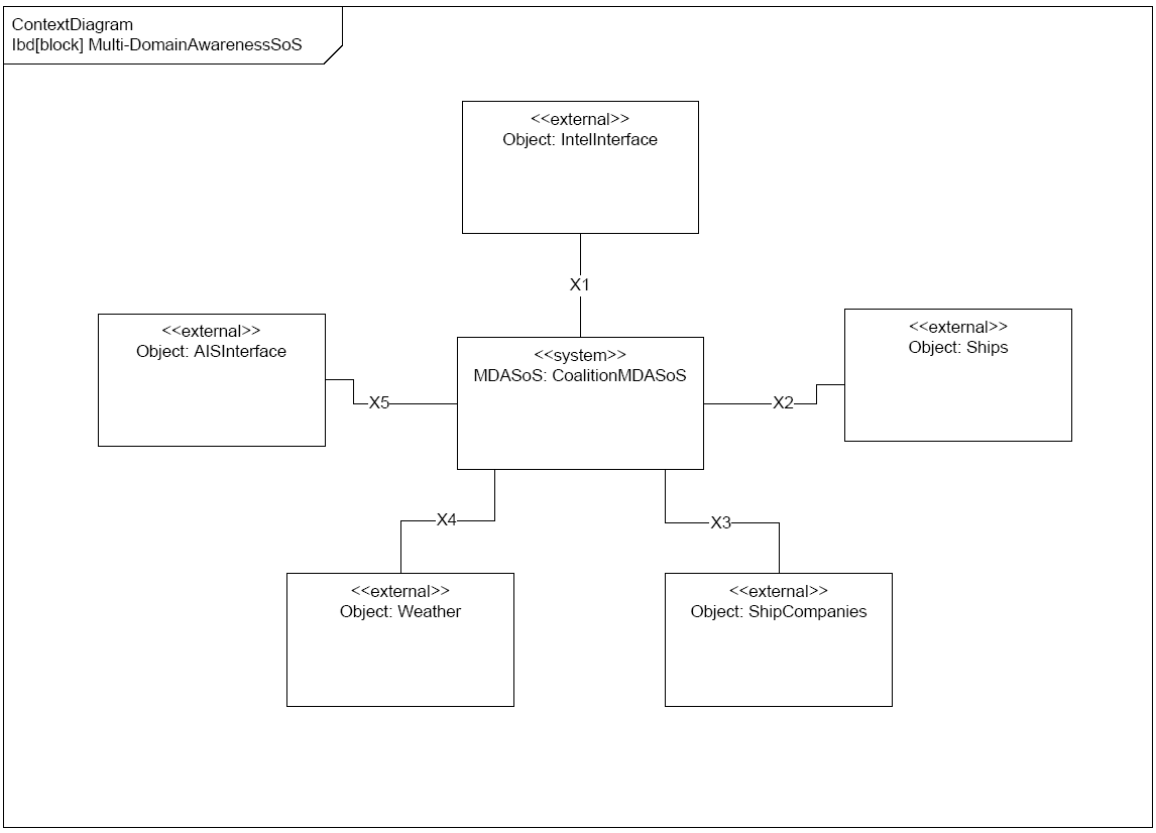

Figure 16. SysML context diagram corresponding to the DoDAF OV-1.

2. Use Case Diagrams

Figure 17 displays the use case diagram for the multi-domain awareness SoS problem description. Triggered by intelligence messages from 'Intel Agency' actor followed by ship manifests from 'Ship Companies' actor, AIS location reports from 'International Maritime Organization' actor, and weather reports from 'Weather Center' actor, the coalition multi-domain awareness SoS performs a sequence of actions indicated by the use cases Receive & Process Intel, Receive & Process Ship Manifests, Fuse Intel & Ship Manifests, Receive & Process AIS Reports, Receive & Process Weather Reports, Process Coalition Sensor Reports & Status, Fuse Sensor, AIS & Weather Reports, Form COP, and Identify & Track Threats.

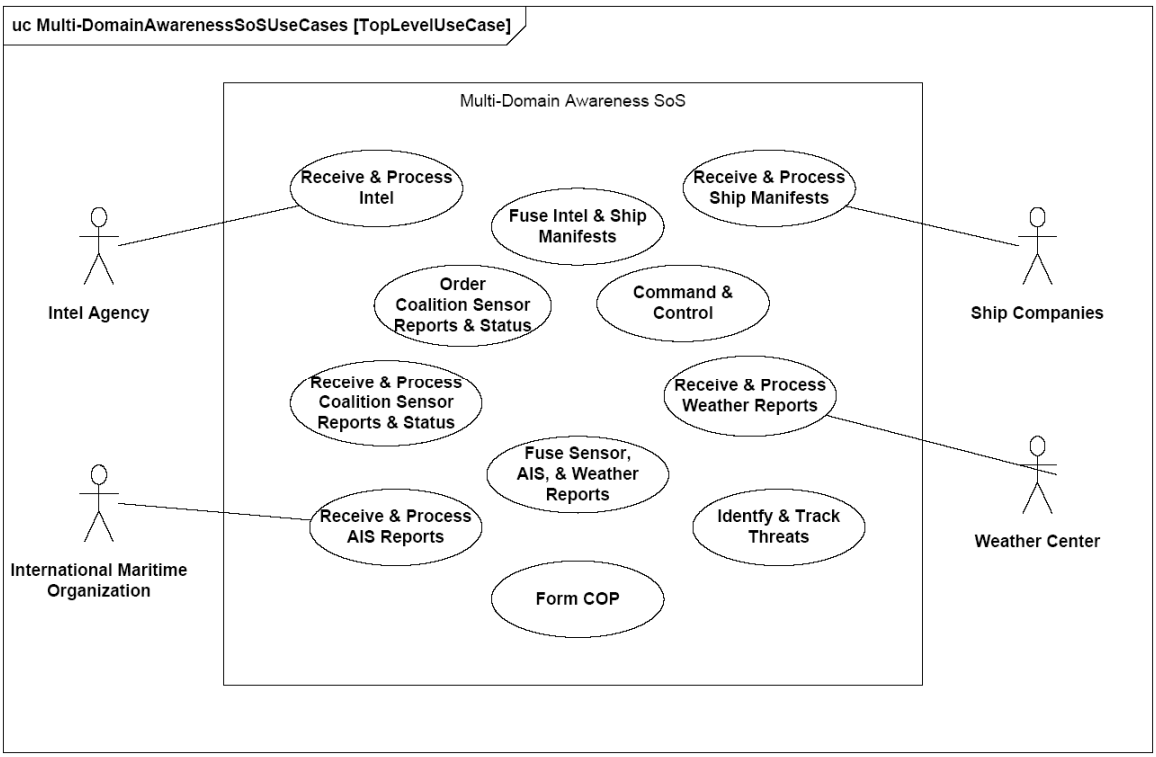

Figure 17. The use case diagram for the multi-domain awareness SoS problem description (DoDAF OV-1 and AV-1)

Figure 18 shows the use case diagram for the Coalition C2. The additional actors are the Australian C2 center, the Canadian C2 center, and the U.S. C2 center, which all provide status and sensor reports to the coalition C2. The Form and Send Alert Messages use case is supported, through <<include>>, by the Process Intel, Process Ship Manifests, and Fuse Intel & Ship Manifests use cases. Likewise, the Formulate and Disseminate COP use case is supported by the Process AIS Reports, Process AUS/CAN/US Sensors Data, Process Weather Reports, Fuse Sensor Data & AIS Reports, and Identify & Track Threats use cases.

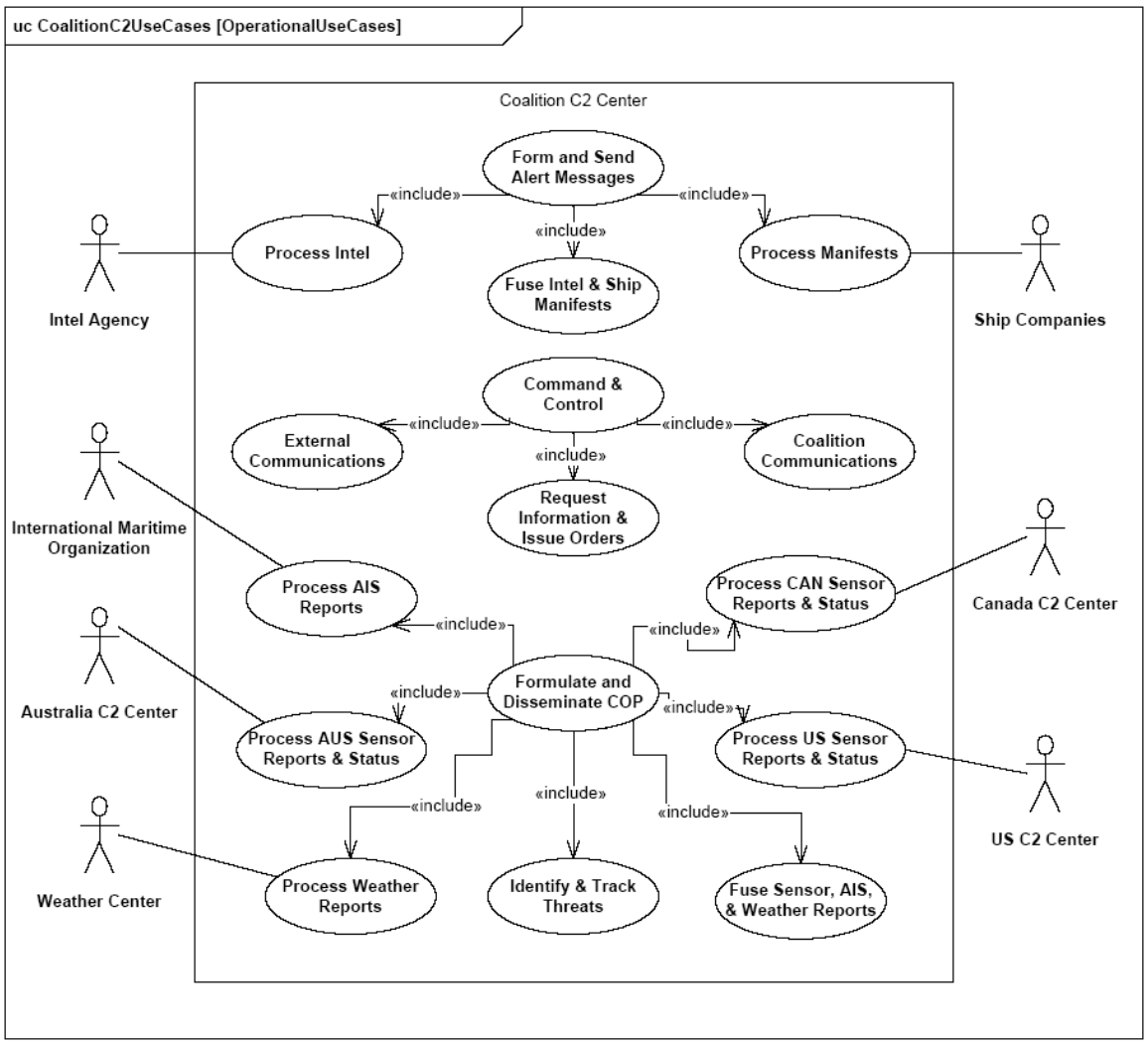

Figure 18. The use case diagram for the 'Coalition AUS-CAN-US C2' (DoDAF OV-1 and AV-1).

3. Requirements Diagrams

The requirements diagram is a SysML diagram type that shows requirements and their relationships to other model elements. For the purposes of illustrating the usage of the SysML requirements diagram, a notional concept of the requirements is developed for the Coalition MDA SoS. Figure 19 is the resulting requirements diagram. As a high-level view of the requirements specification, the requirements diagram shows the trace relationships among Coalition MDA SoS Requirements and a reference to a trade-off analysis that provides the rationale for this trace.

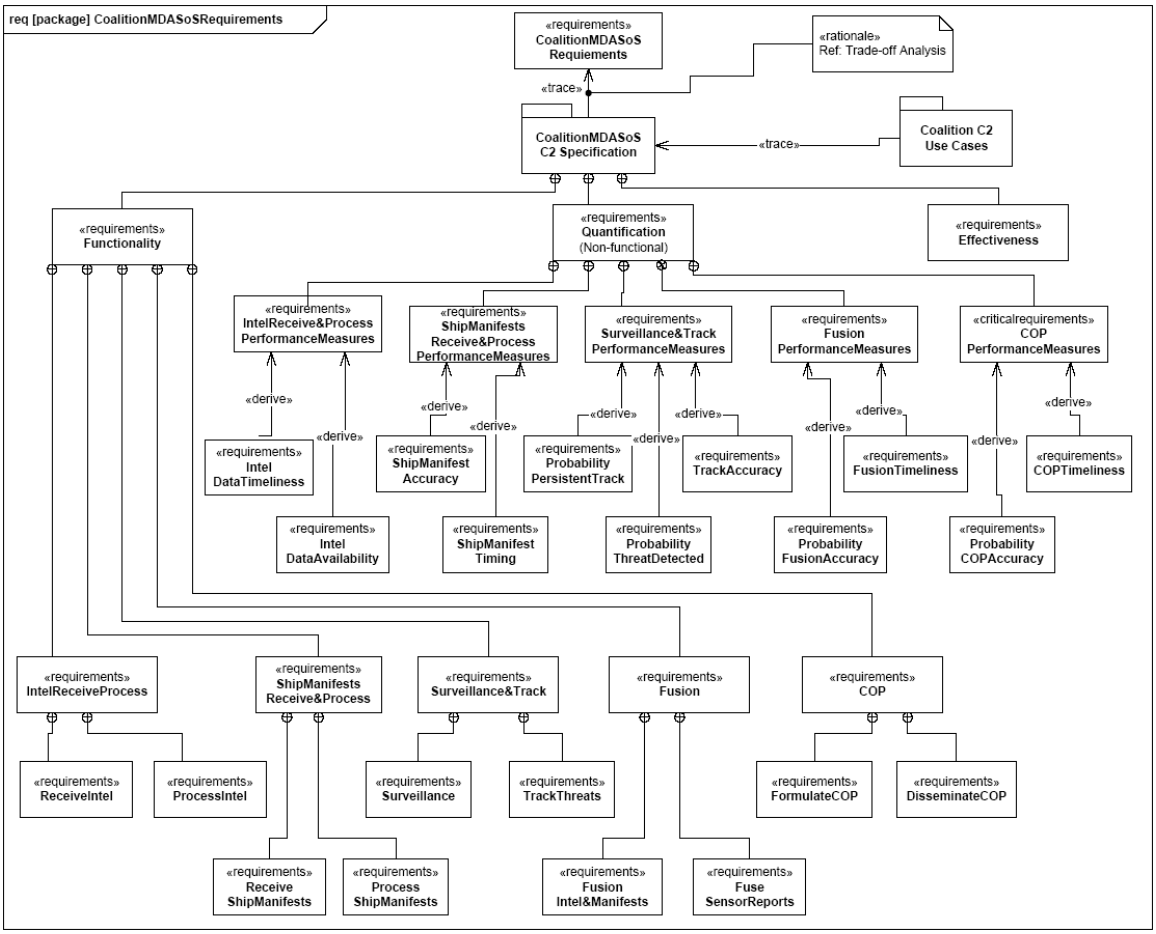

Figure 19. SysML requirements diagram (DoDAF SV-4).

The Coalition MDA SoS specification presumably consists of text requirements. The Coalition MDA SoS Requirements diagram includes the Coalition MDA SoS C2 Specification requirements, functionality is denoted by the stereotype <<requirements>> Functionality, quantification is denoted by the stereotype <<requirements>> Quantification, and effectiveness is denoted by the stereotype <<requirements>> Effectiveness. There are flowdown requirements for each of the top-level requirements. As an example, there are five flowdown requirements for the stereotype <<requirements>> Functionality: IntelReceiveProcess, ShipManifestsReceiveProcess, Surveillance&Track, Fusion, and COP. Figure 19 only includes the requirement flowdown of two top-level requirements due to space considerations.

4. Activity Diagram

The activity diagram for the Coalition MDA SoS depicts the functions that are performed by the various parts of the systems comprising the SoS. As shown in Figures 20 and 21, the SysML activity diagrams allow modeling of the SoS at the functional level. The components of the coalition SoS perform the activities represented by the parts labeled with the functions they perform. The solid lines connecting the ports attached to the various parts show the connectivity and data flow. Both continuous and discrete flows are shown in the diagram.

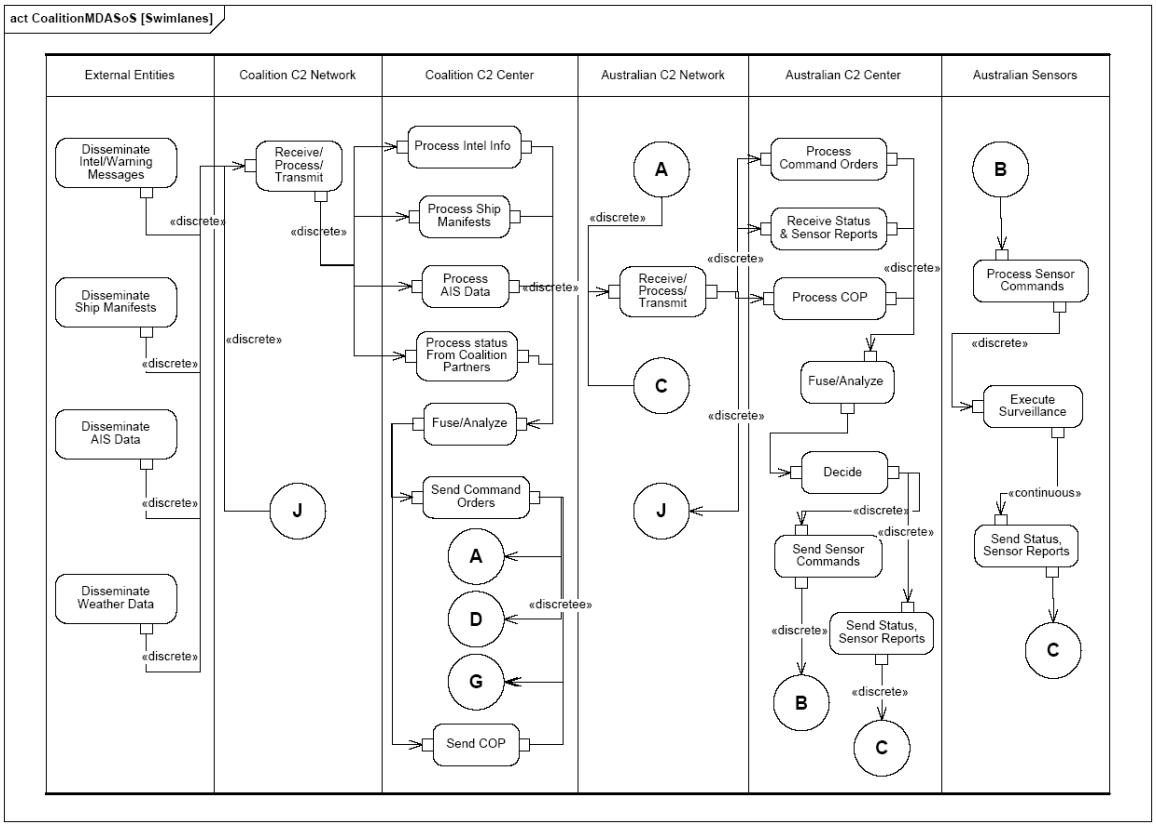

Figure 20. SysML activity diagram, Part 1 of 2 (DoDAF OV-5 and OV-6c).

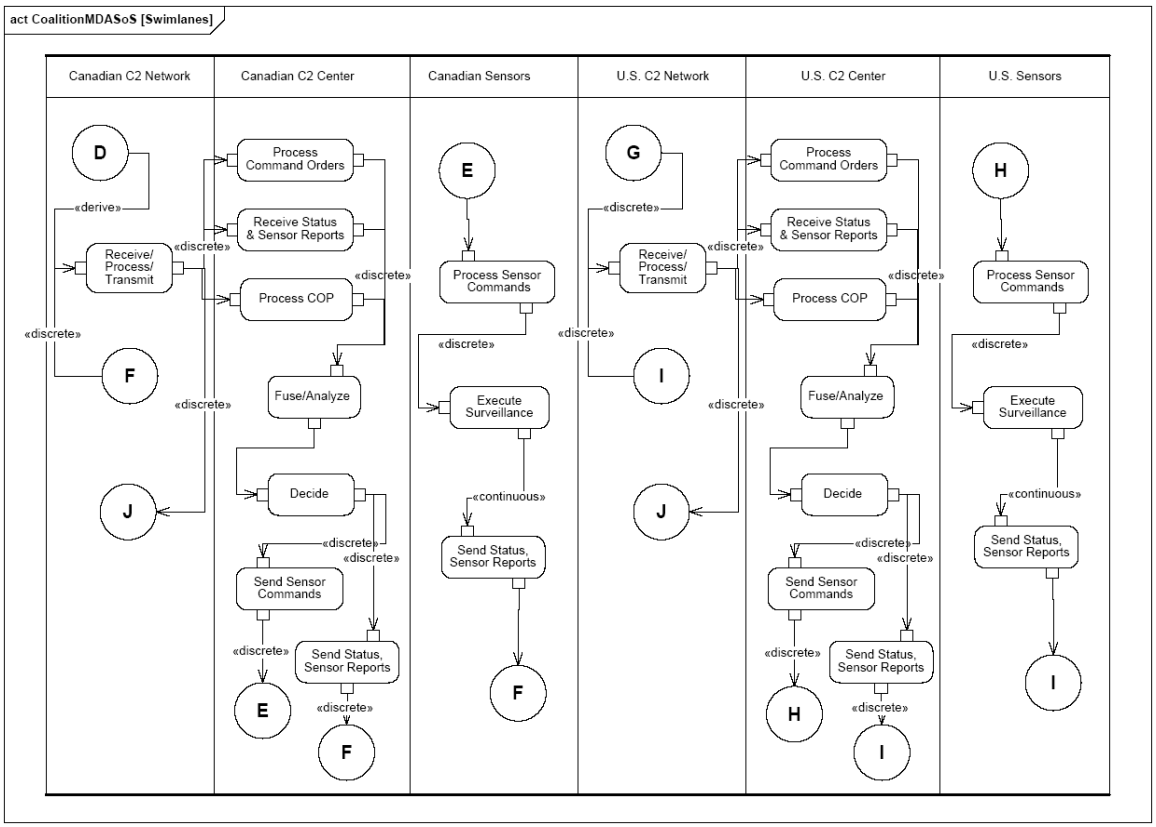

Figure 21. Part 2 of 2, SysML activity diagram (DoDAF OV-5 and OV-6c).

5. Sequence Diagram

The sequence diagram, an example of which is displayed in Figure 22, shows the data/message flows between the different blocks representing the systems within the Coalition MDA SoS and between the Coalition MDA SoS and the systems external to the Coalition MDA SoS. Upon receipt intelligence tip-off of PAVs and possibly ship manifests from ship companies, the coalition C2 disseminates command/alert messages on the coalition network to alert the Australian C2, Canadian C2, and the U.S. C2 centers. Through the Australian C2 network, the Australian C2 center then commands its AP-3C sensors to search for and track the PAVs. Through the Canadian C2 network, the Canadian C2 center commands the RADARSAT sensors to search for and track the PAVs. Through the U.S. C2 network, the U.S. C2 center commands U.S. sensors, both Global Hawk sensors and ship sensors, to search for and track the PAVs. Sensor data (track reports and status) are sent to and processed by each nation's C2 center via its own

respective network. The three C2 centers then send status and processed sensor reports to the Coalition C2 center through the coalition network. The coalition C2 center then processes and fuses the sensor reports producing a COP, which is then sent out to the partner nation C2 centers. The individual C2 centers will use the COP in their response to the PAVs.

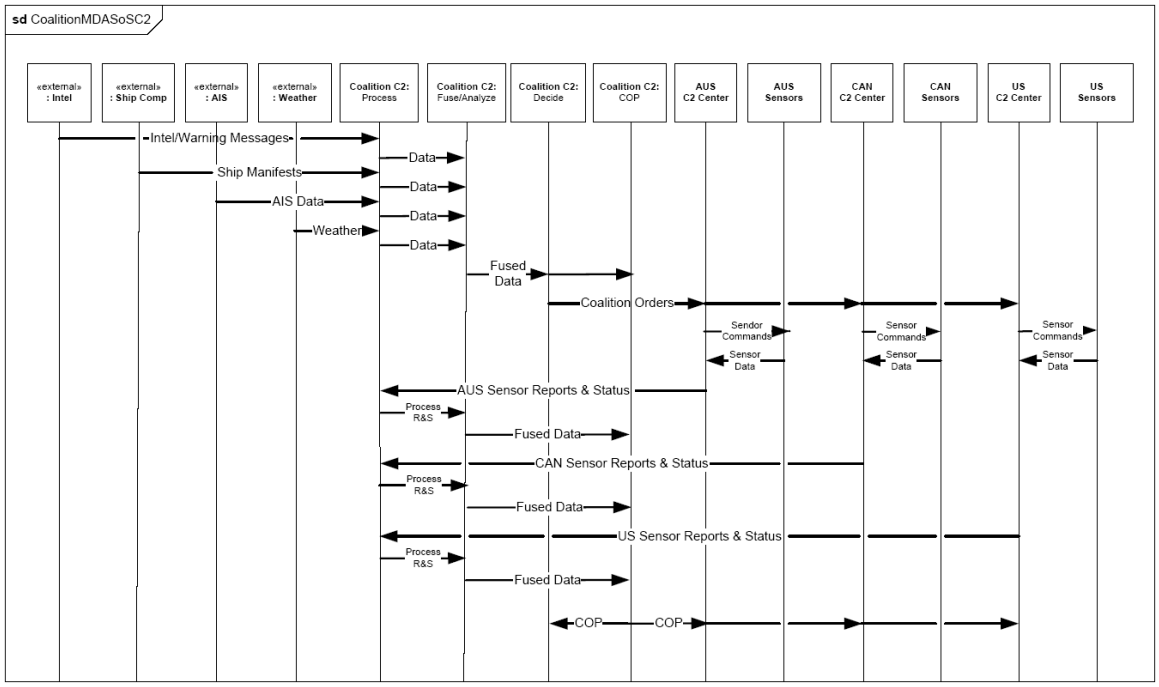

Figure 22. SysML sequence diagram for Coalition MDA SoS C2 (DoDAF SV-1 and OV-6c).

6. Block Breakdown Diagram

Figure 23 shows a top-level SoS composition or the breakdown of the Coalition MDA SoS in terms of the blocks representing the systems of the SoS. The rest of the components in the diagram belong to the SoS and hence are defined using the <<system>> stereotypes. The composition graphical path, connection line with diamond end, indicates the direction of composition among blocks that are composed of other blocks. As an example, the composition graphical paths indicate four separate networks

that compose the MDA SoS networks, four C2 centers that compose the Coalition MDA SoS C2, and the U.S. ship-based radars are from USS Ship 1 and USS Ship 2. The composition graphical path indicates the same scheme for the rest of the blocks.

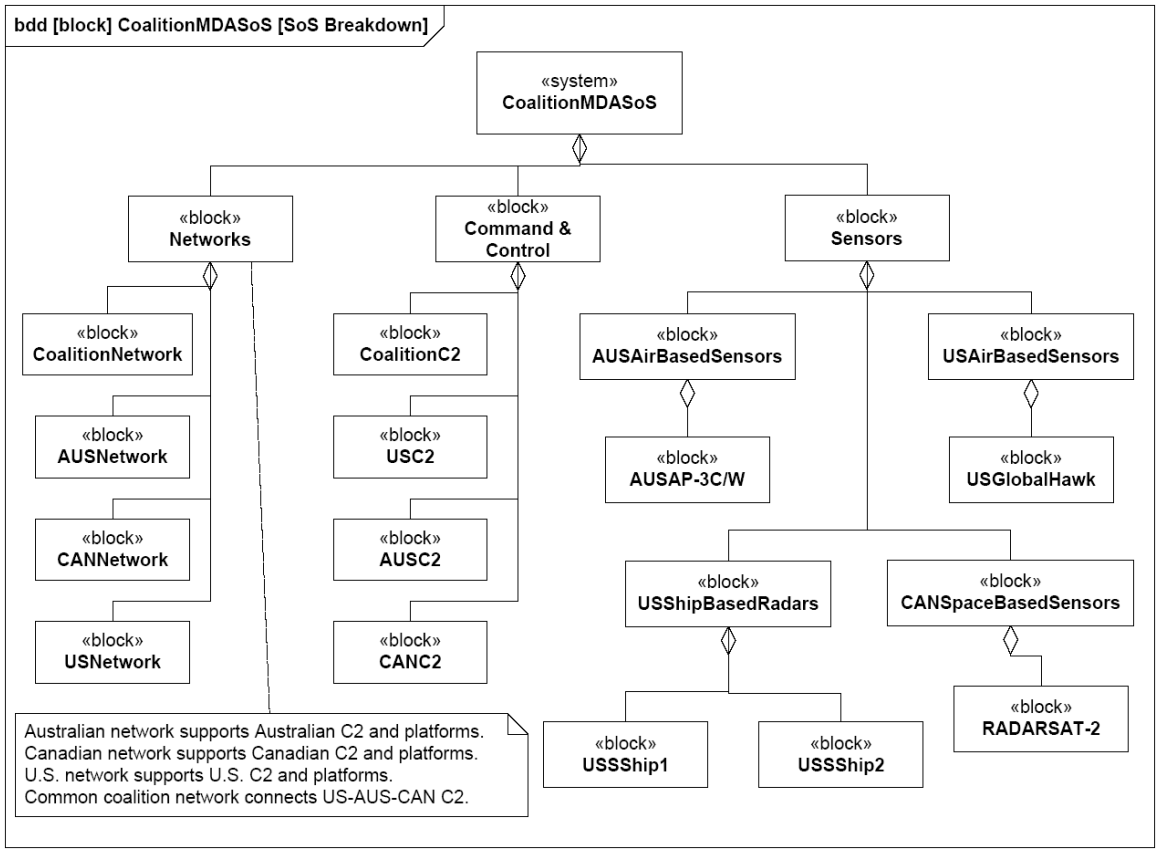

Figure 23. SysML block breakdown diagram depicting composition of the coalition SoS (DoDAF OV-4).

The SysML diagrams presented thus far give a broad representation of the Coalition MDA SoS. Alternative architectures are developed for this Coalition MDA SoS.

C. MDA SOS ALTERNATIVE ARCHITECTURES

The multi-domain awareness SoS concept seeks to exploit information from multiple sources and domains to deliver the situational awareness needed in the maritime domain. Due to the complexity of the MDA SoS, this study identifies and focuses on a system thread, which corresponds to the SysML sequence diagram in Figure 22. The

sequence diagram shows SoS interactions, analogous to a thread in a software system [33]. The SoS interactions begin with initial events from a starting point that trigger a flow of interactions, which prompts subsequent processes in the SoS until an ending point is reached. A further explanation of threads is provided in the simulative study described in Chapter V.

Three architecture alternatives for a multi-domain awareness SoS are considered: a current architecture, a planned architecture using direct tasking, and a conceptual architecture using direct tasking and processing. Each alternative SoS architecture is now explained.

1. Alternative Architecture #1—Current

Figure 24 shows the connectivity of the first alternative SoS architecture. The oval shapes depict the different networks and the solid lines indicate the connections of the different components of the Coalition MDA SoS to a particular network.

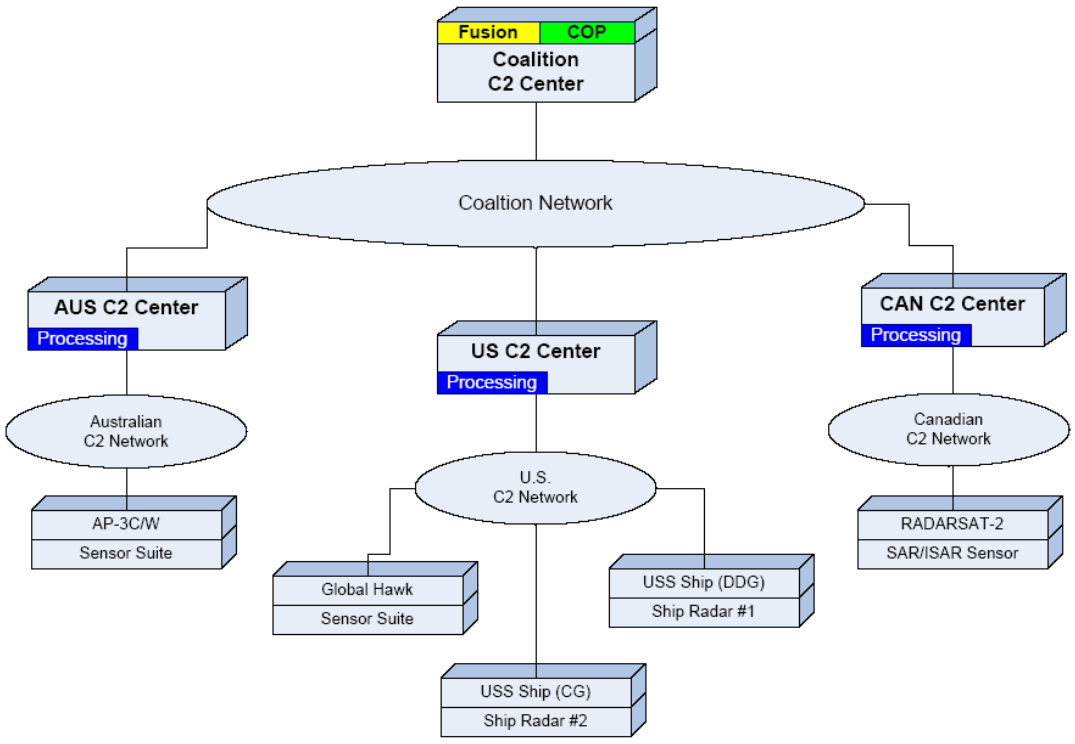

Figure 24. Connections among the different systems of the coalition MDA SoS in Architecture #1.

For example, the Australian AP-3C platform/sensors and the Australian C2 center communicate with each other via the Australian network. The Coalition C2 center communicates with each coalition nation C2 center via the coalition network. However, the Coalition C2 center cannot communicate directly to a coalition nation's platforms/sensors without going through the respective host C2 center. Additionally, in this Coalition MDA SoS architecture, the raw data from coalition nation sensors must be processed in their respective nation C2 center before the processed sensor information is sent to the Coalition C2 center for fusion into the common operational picture.

The sequence diagram for the first alternative SoS architecture (Figure 25) shows the data/message flows between the different blocks representing the systems within the Coalition MDA SoS and between the Coalition MDA SoS and the systems external to the Coalition MDA SoS. The thread in Figure 25 is implemented in modeling during the simulative study.

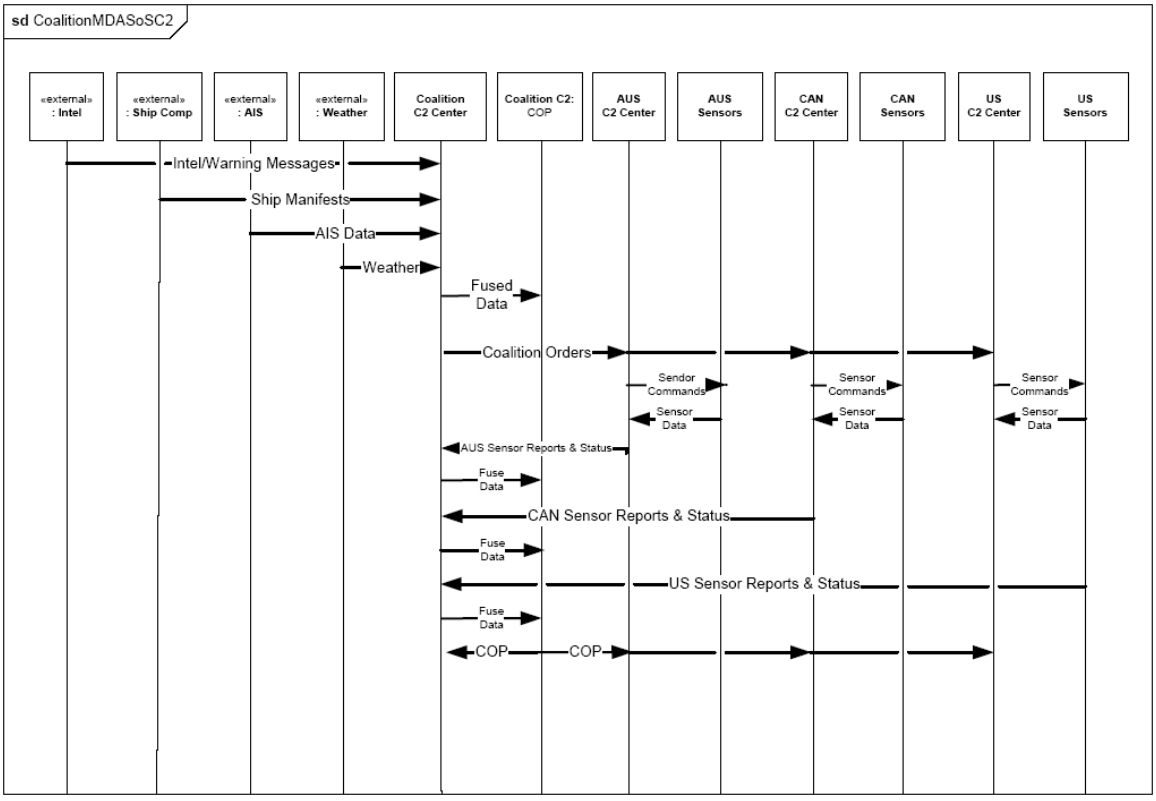

Figure 25. Architecture #1 SysML sequence diagram for Coalition MDA SoS C2.

The Coalition C2 center starts the process upon receipt of an intelligence warning message of a potential maritime attack from the Intelligence Community. The Coalition C2 center requests ship's manifests of PAVs from commercial shipping companies. The AIS and weather data are requested depending on threat location. The Coalition C2 center disseminates command/alert messages via the coalition network alerting the Australian C2, Canadian C2, and the U.S. C2 centers. Through the Australian C2 network, the Australian C2 center then commands its AP-3C sensors to search for and track the PAVs. Through the Canadian C2 network, the Canadian C2 center commands the RADARSAT sensors to search for and track the PAVs. Through the U.S. C2 network, the U.S. C2 center commands U.S. sensors, both Global Hawk sensors and ship sensors, to search for and track the PAVs. Sensor data (track reports and status) are sent to and processed by each nation's respective C2 center via its own network. The coalition nation C2 centers then send status and processed sensor reports to the Coalition C2 center via the coalition network. The Coalition C2 center then fuses the status and sensor reports to produce a COP, which is then disseminated to each coalition nation C2 center. The individual C2 centers will use the COP in their response to the PAVs. The thread ends once the COP is disseminated and received by all C2 centers.

2. Alternative C2 Architecture #2—Planned

The second alternative SoS architecture (Figure 26) is similar to alternative Architecture #1, except the Coalition C2 center can communicate direct tasking assignments to a coalition nation's platforms/sensors without going through the respective host C2 center. This communication flow is one-way only and the raw data from a tasked coalition nation's sensor must still be processed by its respective nation C2 center before the processed sensor information is sent to the Coalition C2 center for fusion. The new communication link is the curved line labeled as "direct tasking," with an arrow showing the direction of communication.

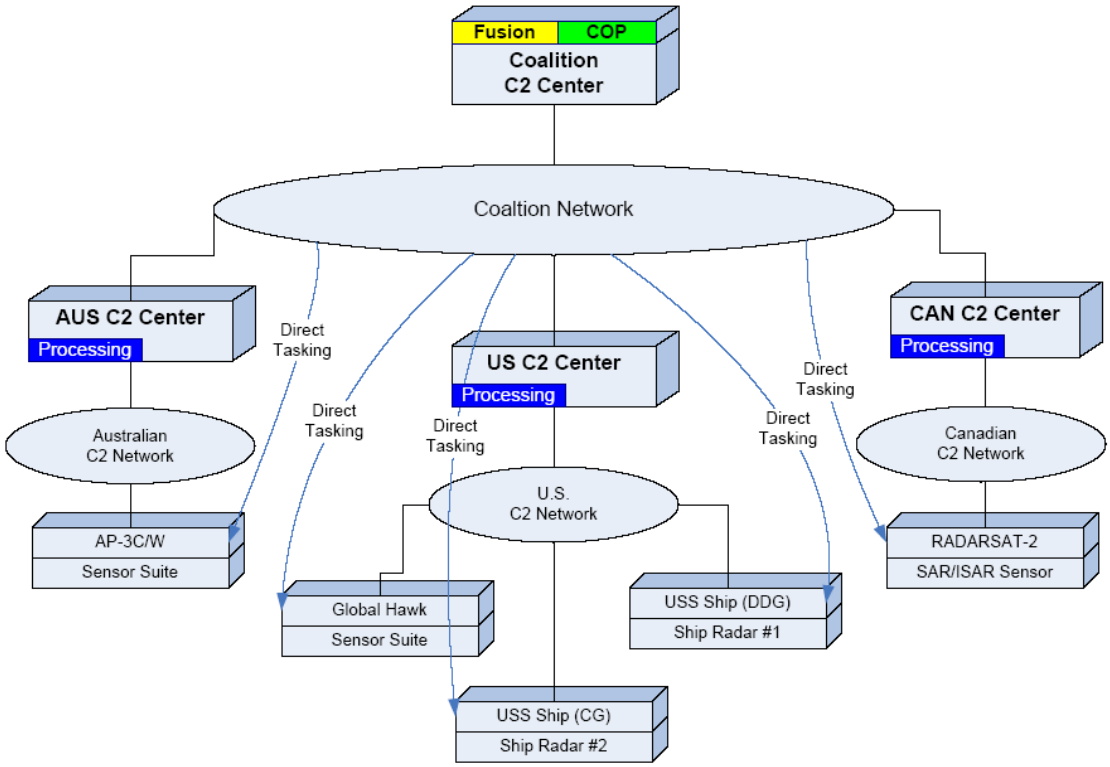

Figure 26. Connections among the different systems of the Coalition MDA SoS in Architecture #2.

The accompanying sequence diagram for the second alternative SoS architecture (Figure 27) shows the data/message flows between the different blocks as described in the first alternative architecture. However, the key difference is the direct tasking sequence from the Coalition C2 center to each platform/sensor, as well as the informational notification to the respective coalition nation C2 centers. The thread in Figure 27 is implemented in modeling during the simulative study.

The Coalition C2 center starts the process upon receipt of an intelligence warning message of a potential maritime attack from the Intelligence Community. The Coalition C2 center requests ship's manifests of PAVs from commercial shipping companies. The AIS and weather data are requested depending on threat location. The Coalition C2 center issues specific tasking orders on the coalition network to the available coalition platforms/sensors to search for and track PAVs. At the same time, alert messages and tasking orders (for information purposes) are sent to the Australian C2, Canadian C2, and

the U.S. C2 centers. Even though the platforms/sensors are directly tasked by the Coalition C2 center, all sensor data (track reports and status) are still sent to and processed by each coalition nation's C2 center via its own network. The coalition nation C2 centers then send status and processed sensor reports to the Coalition C2 center via the coalition network. The Coalition C2 center fuses the status and sensor reports to produce a COP, which is then disseminated to each coalition nation C2 center. The individual C2 centers will use the COP in their response to the PAVs. The thread ends once the COP is received by all C2 centers.

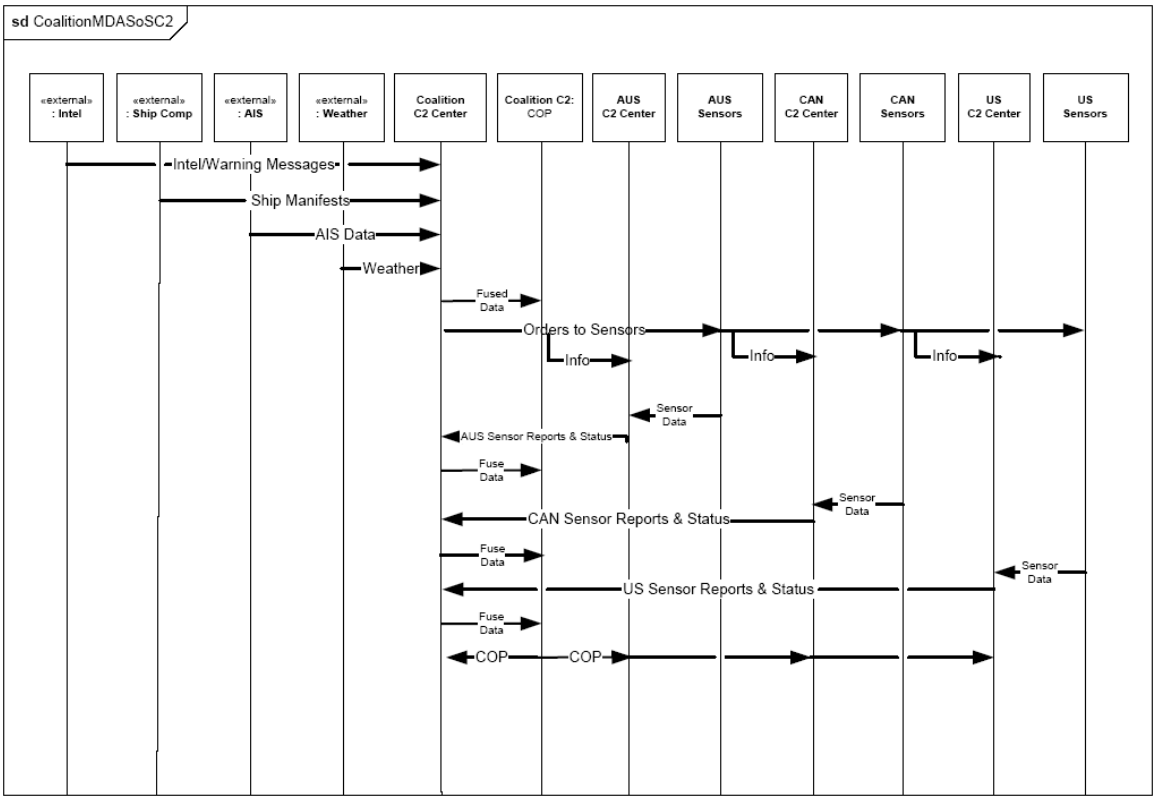

Figure 27. Architecture #2 SysML sequence diagram for Coalition MDA SoS C2.

3. Alternative C2 Architecture #3—Conceptual

The third SoS architecture alternative (Figure 28) is similar to alternative Architecture #2, except that the coalition platforms/sensors have two-way communications with the Coalition C2 center. As shown in Figure 28, the Coalition C2 center has the capability to process sensor data obtained directly from the sensors; the

sensor data thus need not be processed by the respective host C2 center. This alternative architecture eliminates the need for data processing at the coalition nation C2 centers in the MDA SoS. The raw sensor data is subsequently processed by the Coalition C2 center and fused into a COP. A two-way communication link is a double-headed curved line labeled as "direct tasking and reporting."

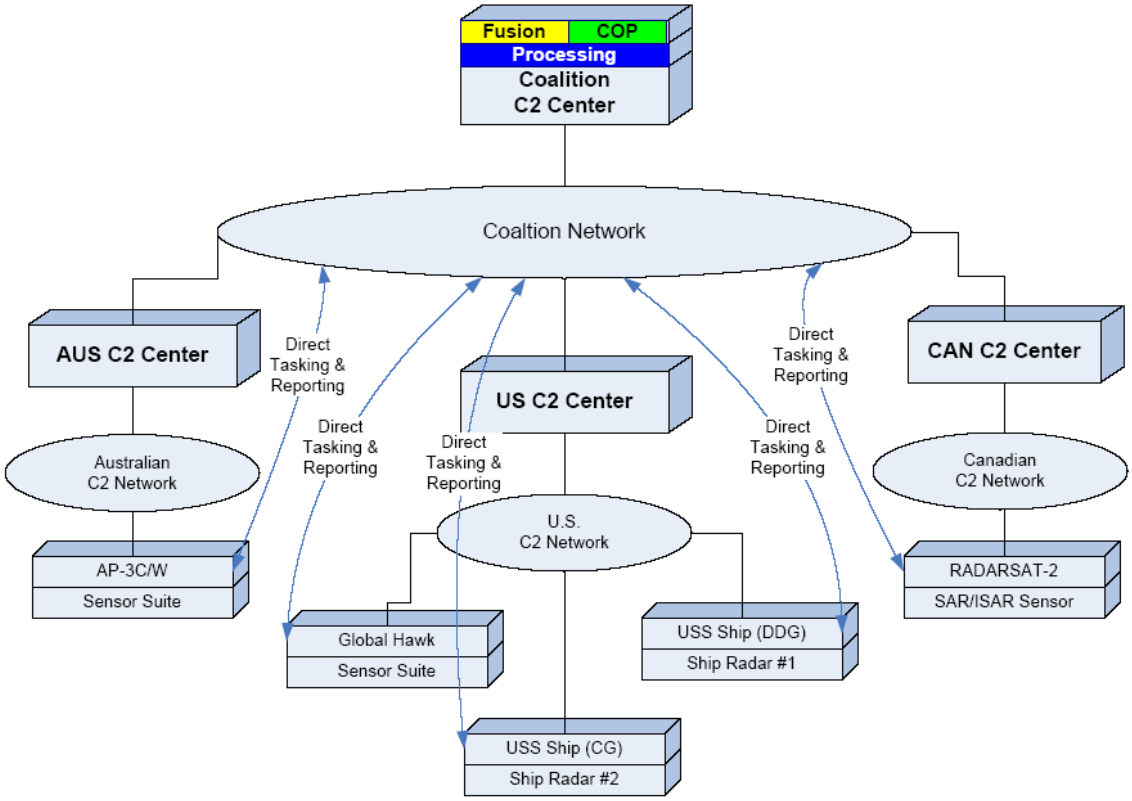

Figure 28. Connections among the different systems of the coalition MDA SoS in Architecture #3.

The sequence diagram for the third SoS architecture alternative (Figure 29) shows the data/message flows between the different blocks as described in the first and second alternative architectures. However, the key difference is the direct tasking and reporting sequence from the Coalition C2 center to each platform/sensor. Notification of tasking is still given to the respective coalition nation C2 centers. The thread in Figure 29 is implemented in modeling during the simulative study.

The Coalition C2 center starts the process upon receipt of an intelligence warning message of a potential maritime attack from the Intelligence Community. The Coalition C2 center requests ship's manifests of PAVs from commercial shipping companies. The AIS and weather data are requested depending on threat location. The Coalition C2 center issues specific tasking orders on the coalition network to the available coalition platforms/sensors to search for and track PAVs. At the same time, alert messages and tasking orders (for information purposes) are sent to the partner nation C2 centers. All sensor data (track reports and status) from tasked platforms/sensors are sent to and processed by the Coalition C2 center via the coalition network. The Coalition C2 center then processes the sensor data, fuses the status and sensor reports, and produces a COP. The COP is then disseminated to each partner nation C2 center. The individual C2 centers will use the COP in their response to the PAVs. The thread ends once the COP is received by all C2 centers.

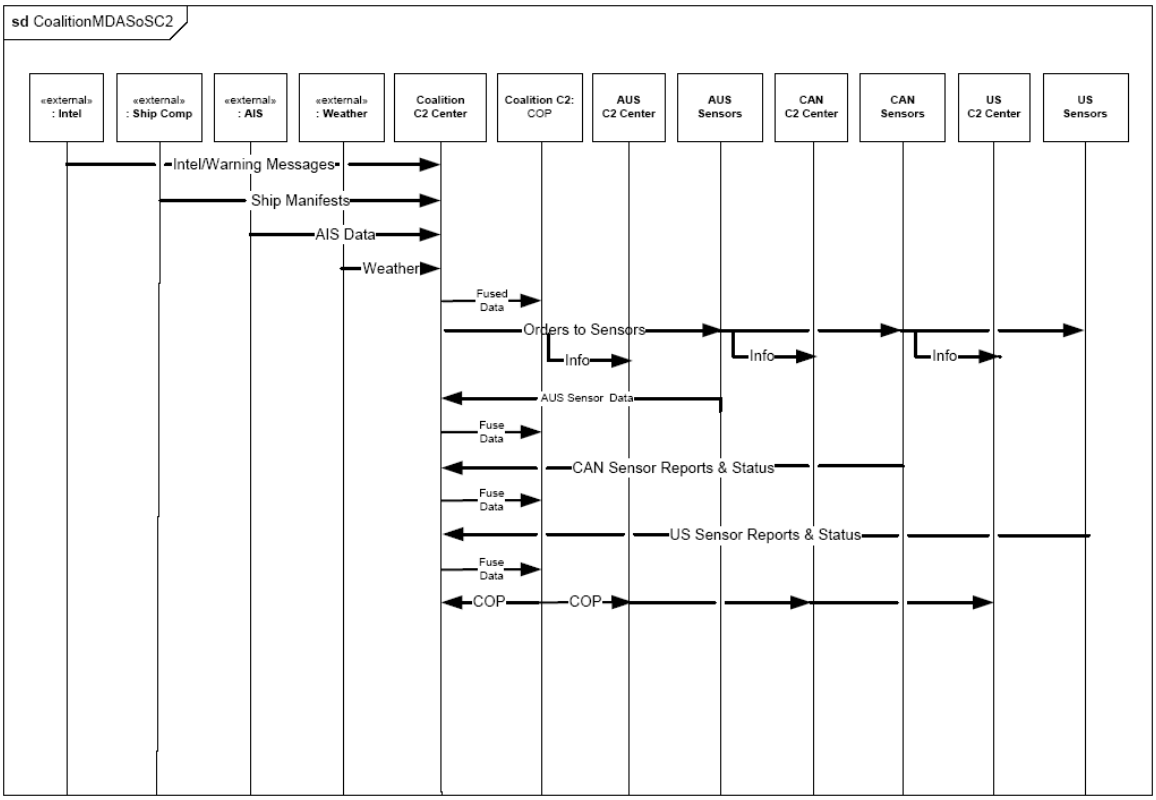

Figure 29. Architecture #3 SysML sequence diagram for Coalition MDA SoS C2.

D. SUMMARY

The integrated systems engineering methodology, discussed in Chapter III, is applied to the coalition multi-domain awareness SoS problem. The SysML diagrams are developed as a representation of the coalition MDA SoS architecture. The selection of three alternative SoS architectures then follows. The three alternative SoS architectures focus on a system thread corresponding to the developed SysML sequence diagram. The sequence diagram shows SoS interactions that begin with an initial event that triggers a flow of interactions until an ending point is reached. The three alternative SoS architectures will be evaluated in the simulative study.

THIS PAGE INTENTIONALLY LEFT BLANK

V. SIMULATIVE STUDY

A. INTRODUCTION

The simulative study, a cornerstone of the SoS Architecture Development Process, provides quantitative measures by which to assess the effectiveness of the alternative SoS architectures. In this simulative study, assessing the effectiveness of the alternative SoS architectures amounts to answering the following questions:

- How much time does it require to establish a COP?
- What is the probability of COP accuracy?

A coalition multi-domain awareness SoS must deliver a timely and accurate COP to support maritime domain awareness. The purpose is to quantify the best SoS performance among the alternative SoS architectures: the current, planned, and conceptual. Modeling and simulation is used to aid in answering these questions.

B. MODELING AND SIMULATION

Modeling is a powerful tool used to analyze, design, and operate complex systems. Models, logical descriptions of how systems perform, are used to assess processes too complex to analyze via spreadsheets or flowcharts. Simulation involves designing a model of a system and conducting experiments on it "to determine how the real system performs and to predict the effect of changes to the system as time progresses" [32].

1. Extend™ Model Development

Extend™ simulation software is used to develop the Coalition MDA SoS C2 model for this simulative study. The simulative study focuses on the system thread that corresponds to the SysML sequence diagram elucidated in Chapter IV.

Three Extend™ models are created, implementing the sequence diagrams for each MDA SoS alternative. In each simulation, the SoS interactions begin with an initial

event from a starting point that triggers a flow of interactions, which prompt subsequent processes in the SoS until an ending point is reached. The starting point for each alternative SoS architecture model is the Intel element, which initiates an intelligence warning alert/message to the Coalition C2 center. The ending point for each alternative SoS model is the point at which the COP is disseminated and received by each of the coalition C2 centers.

The Extend™ models for the simulative study are designed specifically to depict the flow of messages and data that traverse the coalition C2 network for each of the three SoS architecture alternatives. The Extend™ models capture the alternative MDA SoS SysML sequence diagrams in three executable models. The components of the MDA SoS models are now described in detail.

a. Network Model

Figure 30 depicts the top-level module of the coalition C2 network, which is the same for all SoS architecture alternatives. The coalition C2 network model leverages Extend™'s strong hierarchical capabilities, where layers of components are further encapsulated for modularity and organization. For example, encapsulated under the top-level module component known as 'coalition network' are the constructs of the network shown in Figure 31.

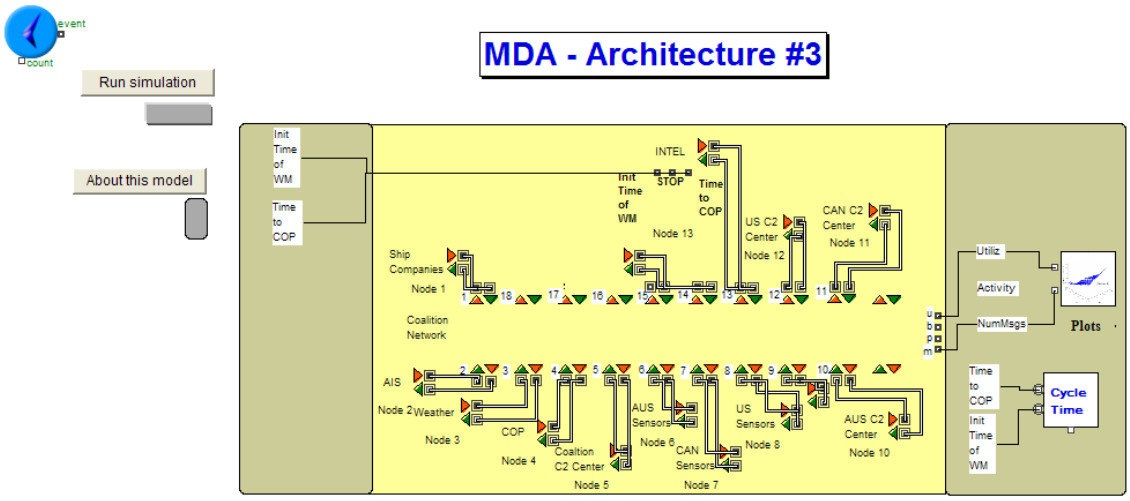

Figure 30. Extend™ top-level view of the Coalition C2 Network model.

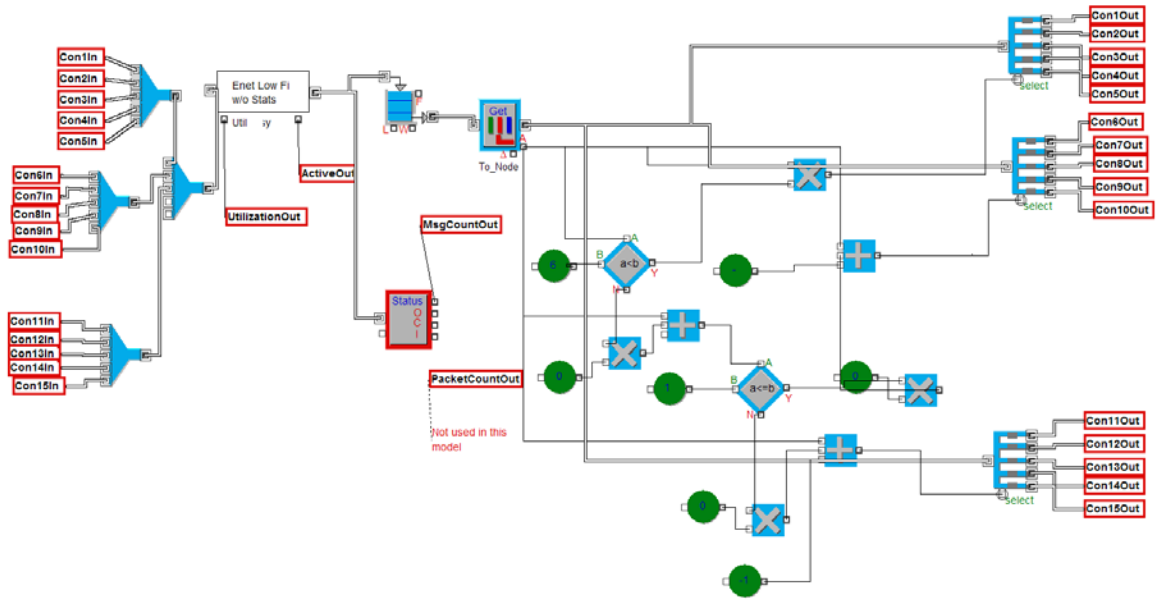

Figure 31. Coalition C2 network modular constructs.

b. Nodes

There are eighteen connectors on the Extend™ coalition C2 network model; however, only twelve connectors are needed for these models. Each of the twelve nodes, which represent the MDA SoS elements, is attached to a connector on the network model. Table 3 shows the SoS elements and their corresponding nodes in the top-level view in Figure 30.

Table 3. List of SoS elements and corresponding nodes in the Coalition MDA SoS model.

SoS Element	Node Number
Intelligence	13
Ship Companies	1
AIS	2
Weather	3
Coalition C2 Center	5
Common Operational Picture	4
Australian C2 Center	10
Australian Sensors	6
Canadian C2 Center	11
Canadian Sensors	7
United States C2 Center	12
United States Sensors	8

Each SoS element in the Extend™ model contains layers of components further encapsulated for modularity purposes. For example, Figure 32 shows part of the Coalition C2 Center element corresponding to node five. The model shown in Figure 32 is used to receive, sort, and reply to messages from other elements in the SoS.

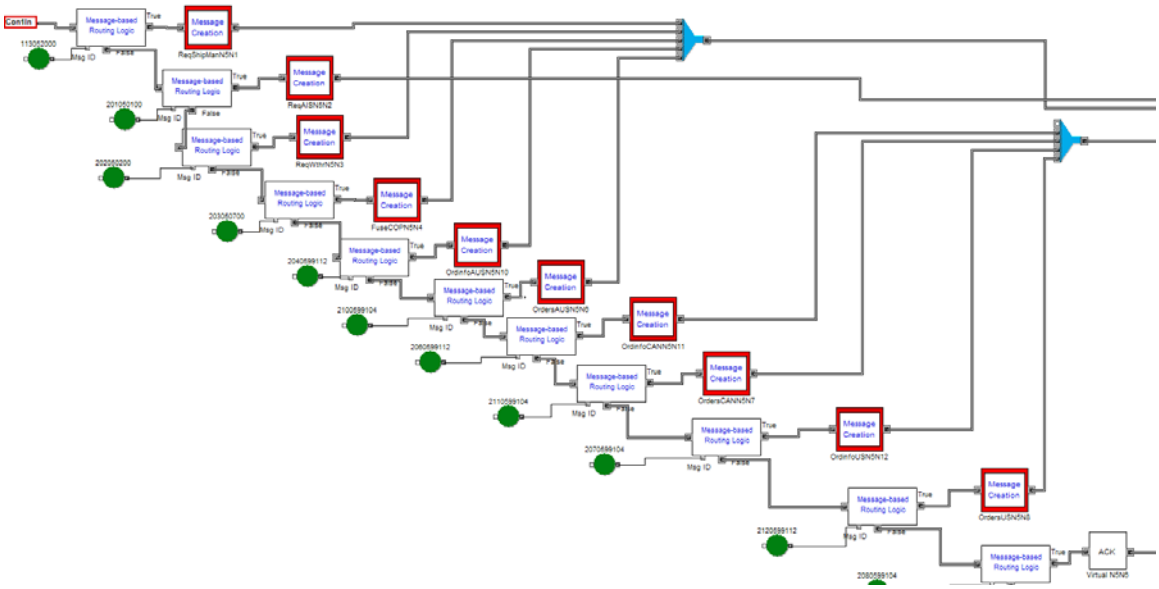

Figure 32. Part of the Coalition C2 center element's message routing decision logic blocks.

Each of the twelve nodes, which represent the SoS elements, have similar message routing and sorting decision blocks, as well as message creation and acknowledgment creation blocks. Figure 33 illustrates how Extend™ models may have embedded blocks in their models. The highest layer in Figure 33 is the Network Node. Each block circled in red is opened to show its contents. The contents of the Message Creation block shows it has a Create Msg Attributes block. The Create Msg Attributes block is opened and shows it contains blocks used to create the attributes of the messages, which will be eventually sent out of this SoS element Node. Some of the message attributes needed for routing are From_Node, To_Node, Msg_Id, Priority, and Msg_Bytes (size).

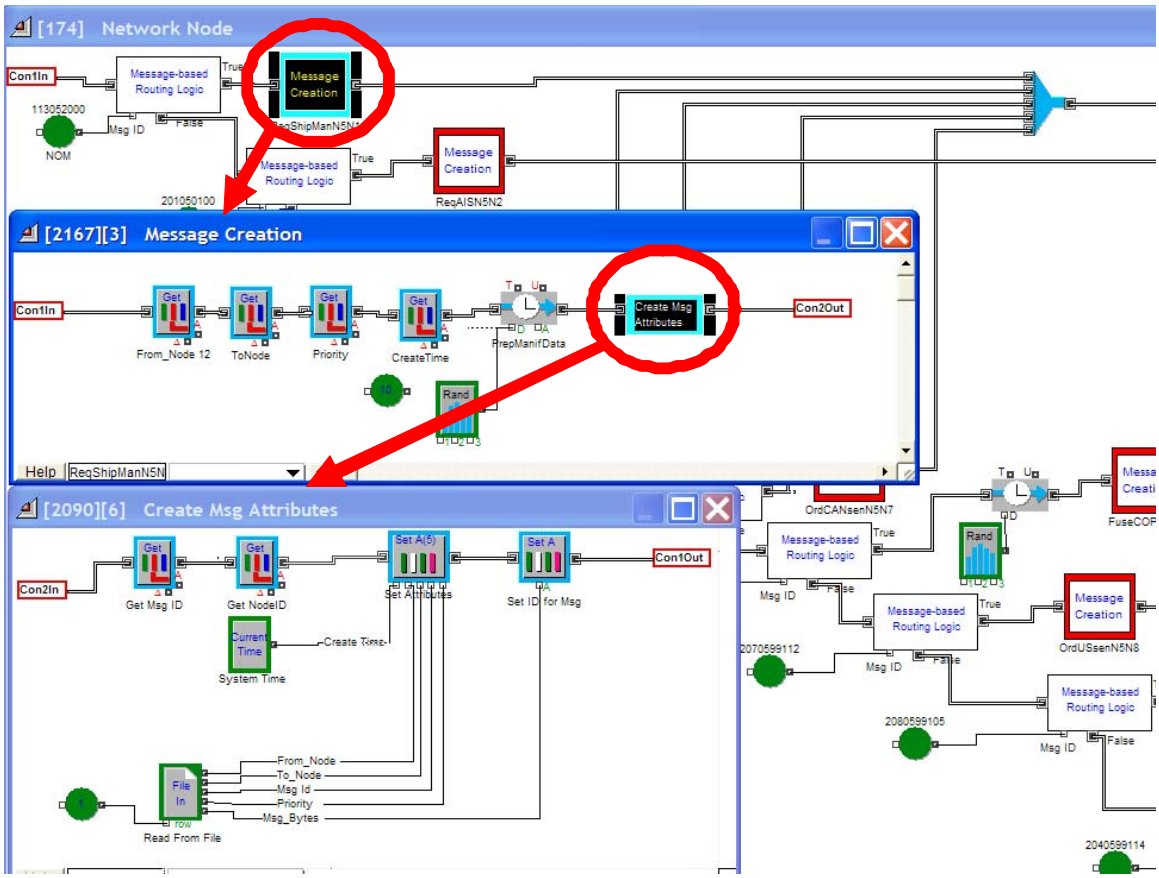

Figure 33. Hierarchical structure breakdown of the Network Node module, showing the Message creation and Create Msg Attributes modules.

Following is the list of other particulars and assumptions of this Coalition MDA SoS Extend™ model:

- The message size varies according to the type of messages. This model uses two main message sizes, Orders/Requests/processed data messages of 40,000 bytes and raw sensor data messages of 400,000 bytes.
- ACK messages are also modeled. Some ACK messages are virtual in the sense that they are not acknowledging messages, but are used to enable simultaneous dissemination of a message. Virtual (ACK) messages keep the flow of the model without incurring any delay.
- A message is characterized by its size, its originator, its destination, and its priority.
- All nodes function in full-duplex mode.
- Every node is connected to the communication network, which is modeled as a LIFO (last in, first out) queue with a constant data rate.

- The model is conducive to Monte Carlo simulation.
- Simulations results can be used for post-processing.

The purpose of this simulative study is to compare the MDA SoS architecture alternatives; therefore, the relative performance of each architecture alternative is of importance, not the detailed numbers used in the construction of the model.

2. Simulation Design

System interactions can be understood by modeling each system in terms of objects corresponding to system elements, with the proper logical flow and timing of items of interest passed between system elements during interactions. Passing of items from one model object to another is analogous to passing messages between objects in SysML diagrams, such as the sequence diagram. In general, the measures of performance of such system of systems include time to complete a thread—such as accomplishing a complex task, or the throughput of items through the total system [33]. Depending on how the model is constructed, another measure of performance could be the quality of the messages or final outputs. In this simulative study, both time to establish a COP and the probability of COP accuracy are used as measures of performance.

a. Time to Establish Common Operating Picture

The first measure of performance is time to establish a COP. Again, each simulation begins with an initial event that triggers all subsequent processes in the SoS thread until an ending point is reached. The starting point for a thread is an intelligence warning alert/message from Intelligence to the Coalition C2 center. The ending point for this thread is the time when the COP is disseminated and received at each coalition nation C2 center. The time to COP completion is the difference between the start time of the initial event (Intel) and the end time of the final event (COP received by all C2 centers).

b. Common Operating Picture Accuracy

The second measure of performance is probability of COP accuracy, denoted by P. Let P_i denote the probability of accuracy of the data from the ith coalition sensor or coalition C2 center. In practice, raw sensor data and/or processed sensor are combined to form a COP. The accuracy of the COP thus depends on that of the raw sensor data and/or processed sensor data. Since this research does not deal with actual raw or processed data from coalition sensors or C2 centers, a probabilistic model of the COP and data accuracy is used. Specifically, the data accuracy from each sensor or C2 center is assumed to follow a uniform distribution, U(0,1), and the probability of COP accuracy is evaluated according to the following simplistic pooling,

$$P = \max_i \left(P_i \right), \tag{1}$$

where *i* denotes the i^{th} source of data.

As seen later in this thesis, $i = 1, 2, 3$ for Architectures #1 and #2, and $i = 1, \cdots, 5$ for Architecture #3. In Architectures #1 and #2, 1 refers to Australia C2 center, 2 to Canada C2 center, and 3 to the U.S. C2 center. In Architecture #3, *i* refers to the total number of sensors in the SoS.

3. Experiment Design and Output

A concern in experimenting with a simulation model for large, complex, interconnected systems is the model's inherent variability. The design of experiments for this simulative study gathers data from 500 simulation runs for each MDA SoS architecture alternative. Figure 34 shows an example of Extend^{TM} time data produced by the simulation runs. The time data is divided into three columns. Column one shows the finish time of the thread, column two shows the start time of the thread, and column three shows the difference between the start and finish times of the thread. The data in the third column are processed and used in assessing the performance differences among the SoS architecture alternatives.

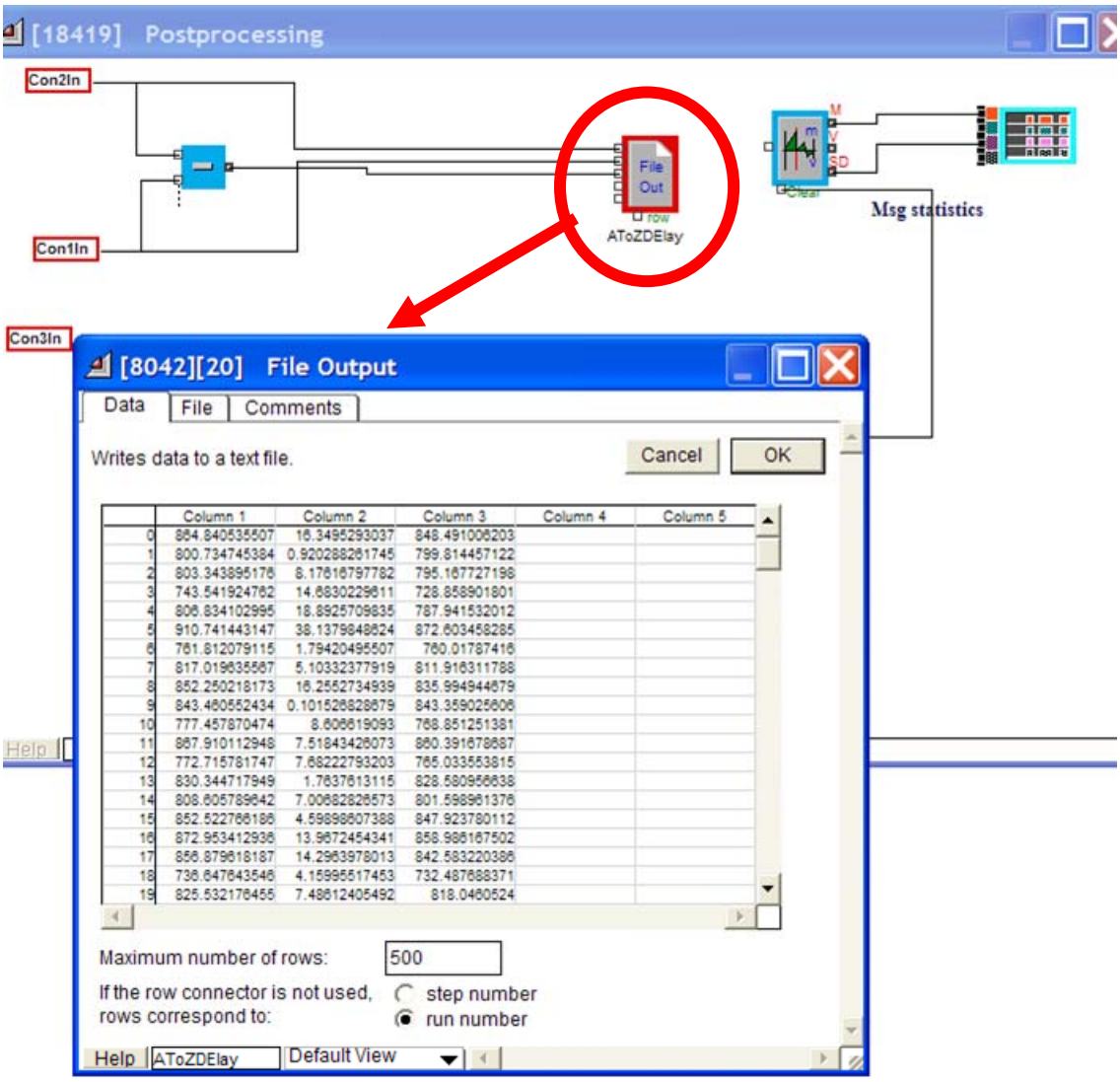

Figure 34. Extend™ model showing collected time outputs for each run. Column one shows finish time, column two shows start time, and column three shows the difference between start and finish times.

The data produced from 500 simulation runs are processed to yield the two measures of performance; namely, the time to establish a COP and the probability of COP accuracy, which will aid in answering the two questions stated in this chapter.

C. DISCUSSION OF RESULTS

1. Time to Establish a Common Operational Picture

Again, the time to establish a COP is measured as the difference between the start time of the initial event and the end time of the final event of a thread. A descriptive statistical analysis is performed on the simulation results, specifically the time needed to complete the sequence of events in the thread (data recorded in column three of Figure 34). Figure 35 compares the statistical results corresponding to the MDA SoS architecture alternatives.

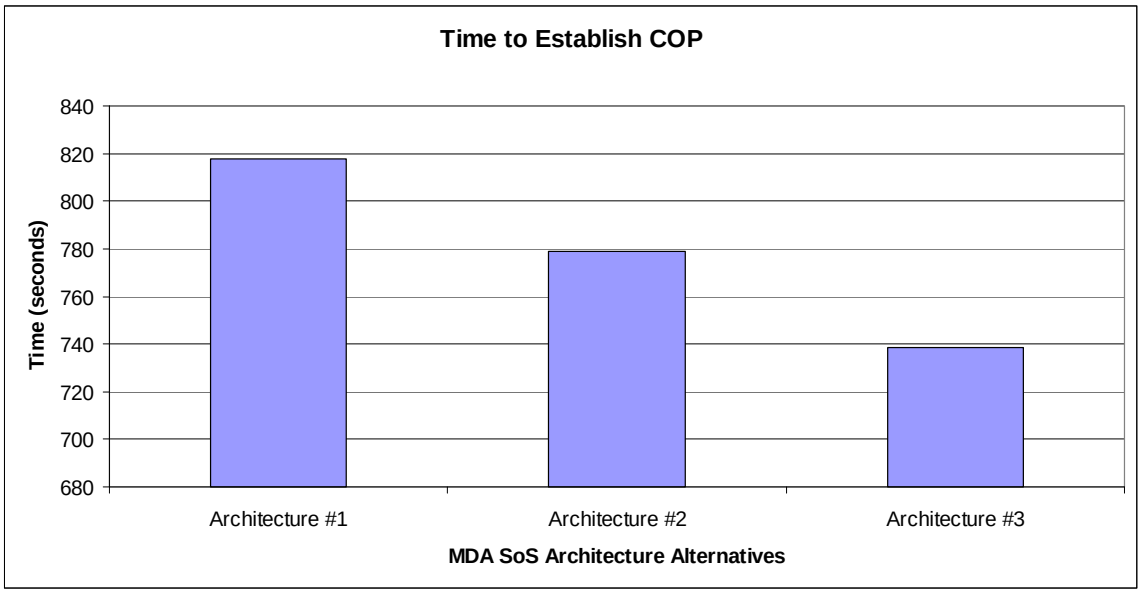

Figure 35. Bar graph displaying the time to establish a COP for MDA SoS architecture alternatives.

Architecture #1, the current architecture, takes the longest time to establish a COP, with a mean time of 818 seconds. Architecture #2, the planned architecture, takes an average time of 779 seconds establishes a COP, which is 4.7% faster than that of the current architecture. The conceptual architecture, Architecture #3, establishing a COP with a mean time of 739 seconds, shows almost a 10% improvement over the current architecture. The MDA SoS architecture that performs best, by taking the least amount of time to establish a COP, is thus Architecture #3.

2. Probability of Common Operational Picture Accuracy

For Architectures #1 and #2, with inputs from the three coalition nation C2 centers—Australia, Canada, and U.S. —using equation (1) and averaging the results from 500 simulation runs result in the probability of COP accuracy of roughly 0.75. For Architecture #3, with inputs from the five sensors—the Australian AP-3C sensor, the Canadian RADARSAT-2 sensor, the U.S. Global Hawk sensor, the U.S. Ship 1 sensor, and the U.S. Ship 2 sensor—again using equation (1) and averaging the results from 500 runs results in probability of COP accuracy of approximately 0.83. Figure 36 compares the accuracy results corresponding to the MDA SoS architecture alternatives.

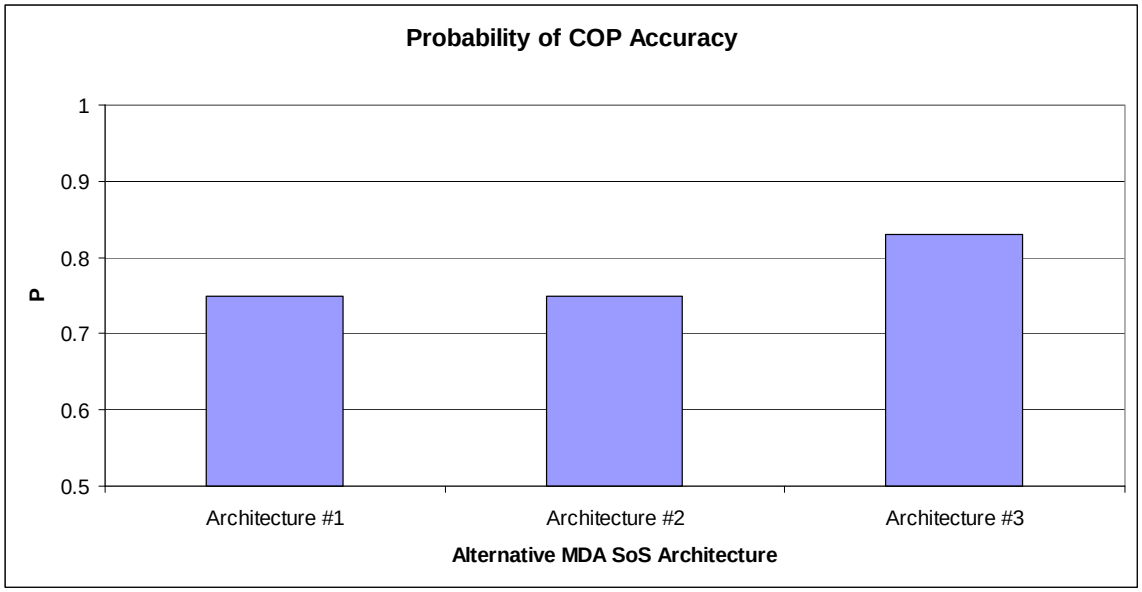

Figure 36. Bar graph displaying the probability of COP accuracy for MDA SoS architecture alternatives.

The first two architectures have the same probability since both architecture alternatives have the same number of data inputs forming the COP. Architecture #3, with a probability of COP accuracy of approximately 0.83, shows almost a 10% improvement over Architectures #1 and #2. The MDA SoS architecture alternative with the highest probability of COP accuracy is Architecture #3.

3. Conclusion

Based on the results of the two measures of performance, the best alternative MDA SoS architecture is Architecture #3. Architecture #3's time to establish COP is 10% faster than that of Architecture #1 and 5% faster than that of Architecture #2. Additionally, Architecture #3's probability of COP accuracy is higher than those of both Architectures #1 and #2. Based on the two tested measures of performance, the MDA SoS architecture alternative's ranking, in a decreasing order, are: Architecture #3, Architecture #2, and Architecture #1.

D. SUMMARY

This chapter describes the simulative study using modeling and simulation. It describes the use of the Extend^{TM} simulation software employed in this research to develop the alternative MDA SoS architecture models. The development of the models and the experiment design are then described in detail. A statistical analysis is performed on the Extend^{TM} simulation results to identify the best-performance SoS architecture for each measure of performance. Architecture #3 is found to be the best architecture, taking the least time to establish a COP with the greatest probability of COP accuracy.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS AND FUTURE RESEARCH

A. INTRODUCTION

This chapter presents the conclusions, key findings, and areas for future research. Section B summarizes the research. Section C captures the key findings. Section D discusses areas for future research. Finally, Section E concludes the thesis.

B. RESEARCH SUMMARY

The research conducted in this thesis applies a systems engineering approach to answering the research question: What is the best NCO SoS architecture for MDA? This question shapes the research and analysis accomplished in this thesis.

The research begins by defining the multi-domain awareness problem, background, the coalition multi-domain awareness SoS problem statement, and scenario. It then applies the integrated systems engineering methodology for analyzing and ranking SoS architectures [3] to the coalition multi-domain awareness SoS problem. SysML diagrams are developed to represent three coalition multi-domain awareness SoS architectures, which are evaluated in the simulative study using modeling and simulation. Extend^{TM} software is used to develop the alternative MDA SoS architecture models for the simulative study. The experiment design is then performed to evaluate the MDA SoS architecture alternatives. The simulation results are processed to produce the measures of performance for each MDA SoS architecture alternative, which are the time to establish COP and the probability of COP accuracy. A statistical analysis is then conducted on the results to determine the best MDA SoS architecture. The best MDA SoS architecture provides the most accurate COP in the least time.

C. KEY FINDINGS

The key findings from the research conducted in this thesis follow.

In general, in a highly distributed network, which is the backbone of net-centric operations, the resulting connectivity of the network would allow direct or assured communications with reduced delay between any two nodes of the network, provided that there is no bottleneck resulting from lack of sufficient bandwidth on any communications link. In particular, in the distributed network of Architecture #3, direct links between the sensors and the coalition C2 center shorten the communications delay, and hence, reduce the time to establish a COP.

The integrated systems engineering methodology for analyzing SoS architectures provides an effective framework and tool for designing and analyzing complex SoS in general and NCO MDA SoS in particular. Architecture representations using SysML activity and sequence diagrams aid in identifying and resolving some modeling and SoS interoperability issues, such as communications and concepts of operations. Furthermore, modeling the threads (i.e., sequences of events), based on these SysML diagrams, aids in understanding the NCO MDA SoS behavior. Finally, the simulative study has been found to be an effective tool for assessing the performance of the SoS architectures and for ranking the SoS architectures.

D. AREAS FOR FUTURE RESEARCH

Multi-domain awareness has emerged as a high priority mission area for the Department of Defense and the Department of Homeland Security. The problem scenario, assumptions, and results of this research reflect only an instance of a complex MDA problem. All of the models employed in this research are created with variable inputs that can be changed to suit other situations or scenarios. The approach and analysis used in this research, coupled with the adaptability of the models, provide future researchers with a tool to use for future analysis of NCO multi-domain awareness systems of systems.

In light of the possibility of terrorist activities, accidents, and natural disasters, the multi-domain awareness problem addressed in this thesis spawns a number of areas for future study and research, such as:

- Architecting an NCO SoS architecture that integrates current capabilities and legacy systems into an interoperable organization of sensors, data, information, intelligence, and dissemination tools and processes for a national MDA capability.
- Applying space-based radar specifically for open-ocean coverage and integrating the space-based radar data with AIS to identify anomalous activity as a means for cueing less costly surveillance assets.
- Developing resource allocation and optimization algorithms for cost effective use of sensors and processing resources.
- Implementing a simulation to assess an optimal number and type of sensors to determine their impact on the performance of an NCO MDA SoS.
- Implementing a simulation to assess the SoS impact and performance in various geographic areas and environments.
- Assessing the distributed or common operational picture capabilities among MDA fusion centers and existing national and regional fusion centers in order to improve their combined capabilities in a joint or coalition MDA mission.

E. CONCLUSION

This thesis applies the integrated systems engineering methodology for analyzing architectures of SoS [3] for multi-domain awareness. The integrated systems engineering methodology, developed at the Naval Postgraduate School, involves linking the SoSADP to the DoDAF products, using SysML diagrams to represent and model DoDAF products, and hence, to model the SoS architectures, and linking the SysML diagrams to SoSADP via executable simulation models. Focusing on an NCO multi-domain awareness SoS architecture, this research selects the best SoS architecture through applying the integrated systems engineering methodology with an exploratory application to analysis of a coalition MDA SoS C2 architecture employed to aid in countering terrorism emanating from the maritime domain.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] National Strategy for Maritime Security: National Plan to Achieve Maritime Domain Awareness, 2005.

[2] C.A. Clark, The Economics Impact of Nuclear Terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability, Cambridge, MA, April 30, 2003. http://abtassociates.com/reports/ES-Economic_Impact_of_Nuclear_Terrorist_Attacks.pdf (accessed June 2008).

[3] T.V. Huynh and J.S. Osmundson, "An Integrated Systems Engineering Methodology for Analyzing Systems of Systems Architectures," Asia-Pacific Systems Engineering Conference, Singapore, March 23-24, 2007.

[4] Department of Defense Architecture Framework (DoDAF), Version 1.5, April 23, 2007, http://dars1.army.mil/IER/index.jsp (accessed May 2008).

[5] SysML Partners, OMG SysML Specification (OMG SysMLTM), v. 1.0, September 2007, http://www.sysml.org/specs.htm (accessed July 2008).

[6] Johns Hopkins University Applied Physics Laboratory website, http://www.jhuapl.edu/newscenter/aplnews/2004/summer_mda.asp (accessed September 2008).

[7] CRS Report for Congress (CRS Order Code RL32411), Network Centric Operations: Background and Oversight Issues for Congress, updated March 15, 2007.

[8] Joint Chiefs of Staff, Joint Vision 2010, Washington, D.C., 1996.

[9] Joint Chiefs of Staff, Joint Vision 2020, Washington, D.C., June 2000.

[10] NST/NRC, Network-Centric Naval Forces: A Transition Strategy for Enhancing Operational Capabilities Overview, National Academy Press, Washington D.C., 2000.

[11] P.J. Butler, "Project Polar Epsilon: Joint Space-Based Wide Area Surveillance and Support Capability," Director of Space Development, National Defence Headquarters, Ottawa, Canada, 2007.

[12] Open Geospacial Consortium, OGC Web Services (OWS) in Support of the C4ISR Enterprise, version 1.0, November 26, 2007.

[13] Australian AP-3C picture, http://search.janes.com/Search/imageDocView.do?docId=/content1/janesdata/captions/jni/history/jni2003/jni00681_2.htm@captions&keyword=raaf&backPath=http://search.janes.com/Search&Prod_Name=JNI& (accessed September 2008).

[14] Canadian RADARSAT-2 picture, http://www.ec.gc.ca/EnviroZine/images/Issue78/RADARSAT2_l.jpg (accessed September 2008).

[15] USAF Global Hawk picture, http://www.airforce-technology.com/projects/global/images/4_global_hawk.jpg (accessed September 2008)

[16] USS Monterey (CG 61) picture, http://upload.wikimedia.org/wikipedia/commons/f/f7/USS_Monterey_%28CG-61%29_at_sea.jpg (accessed September 2008).

[17] USS Pinkney (DDG 91) picture, http://www.navysite.de/dd/ddg91.htm (accessed September 2008).

[18] United States Intelligence Community website, http://www.intelligence.gov/1-definition.shtml (accessed August 2008).

[19] M. Eidus, Presentation for "Space-Based Radar Exploitation and Data Fusion for Maritime ISR," DEMC Conference, Vantage Point International Inc., April 27, 2006. http://www.esricanada.com/documents/User_Presentation_Space_Based_Radar_Exploitation_and_Data_Fusion_for_Maritime_ISR.pdf (accessed August 2008).

[20] Lloyd's MIU website, http://www.lloydsmiu.com/lmiu/index.htm (accessed August 2008).

[21] J.S. Osmundson, R. Gottfried, Y.K. Chee, H.B. Lau, W. L. Lim, P.S.W. Poh, and C.T. Tan, "Process Modeling: A Systems Engineering Tool for Analyzing Complex Systems," Systems Engineering, vol. 7, no. 4, pp. 320-337, 2004.

[22] J.S. Osmundson and T.V. Huynh, "A Systems Engineering Methodology for Analyzing Systems of Systems," Proceedings of 1st Annual System of Systems Engineering Conference, Johnstown, PA, June 13-14, 2005, http://www.sosece.org (accessed June 2008).

[23] T.V. Huynh and J.S. Osmundson, "A Systems Engineering Methodology for Analyzing Systems of Systems Using Systems Modeling Language (SysML)," Proceedings from the 2nd Annual System of Systems Engineering Conference, Ft. Belvoir, VA, sponsored by the National Defense Industrial Association (NDIA) and OUSD AT&L, July 25-26, 2006, http://www.sosece.org (accessed July 2008).

[24] Defense Acquisition University, Defense Acquisition Guidebook, Defense Acquisition University, Washington, D.C., 2007. https://akss.dau.mil/DAG/Guidebook/IG_c4.2.6.asp (accessed September 2008).

[25] M. Hause and F. Thom, Rebuilding the Tower of Babel—The Case for UML with Real-time Extensions, INCOSE Spring Symposium, May 14-16, 2001.

[26] M.S. Rao, Ramakrishnan, and C. Dagli, Modeling Net-centric System of Systems Using the Systems Modeling Language, Proceedings of the Fourth Annual Conference on Systems Engineering Research, Los Angeles, CA, April 7-8, 2006.

[27] D.E. Wisnosky, et al., DoDAF Wizdom, Wizdom Systems, Inc., 2004.

[28] Department of Defense, DoD Architecture Framework, Version 1.5, Volume I: Definitions and Guidelines, April 23, 2007.

[29] IEEE STD 1471-2000, Recommended Practice for Architecture Description of Software-Intensive Systems, http://www.iso-architecture.org/ieee-1471-faq.html (accessed September 2008).

[30] Department of Defense, DoD Architecture Framework, Version 1.5, Volume II: Product Descriptions, April 23, 2007.

[31] G. Thomas, Presentation for "Civilian Space for Maritime Domain Awareness," University of Miami, 2007, http://www.oceanusmeeting.com/mda/documents/Breakout_Group_Instructions_Support_Civilian-Space-Systems-for-MDA.pdf (accessed August 2008)

[32] D. Farris, Extend 6: Program Overview, webpage http://www.gtpcc.org/gtpcc/extend6.htm (accessed July 2008).

[33] J. Osmundson, N. Irvine, G. Schacher, J. Jenson, G. Langford, T. Huynh, and R. Kimmel, "Application of System of Systems Engineering Methodology to Study of Joint Military Systems Interoperability," Proceedings from the 2nd Annual System of Systems Engineering Conference, Ft. Belvoir, VA, sponsored by the National Defense Industrial Association (NDIA) and OUSD AT&L, July 25-26, 2006, http://www.sosece.org (accessed July 2008).

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California